世界知的所有権機関
国際事務局

PCT

特許協力条約に基づいて公開された国際出願

(51) 国際特許分類7 H04N 1/40, 1/387	A1	(11) 国際公開番号 WO00/51338 (43) 国際公開日 2000年8月31日(31.08.00)

(21) 国際出願番号 PCT/JP00/01097
(22) 国際出願日 2000年2月25日(25.02.00)
(30) 優先権データ
特願平11/49996 1999年2月26日(26.02.99) JP
特願平11/49997 1999年2月26日(26.02.99) JP

(71) 出願人（米国を除くすべての指定国について）
松下電器産業株式会社
(MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.)
[JP/JP]
〒571-0050 大阪府門真市大字門真1006番地 Osaka, (JP)
(72) 発明者；および
(75) 発明者／出願人（米国についてのみ）
小嶋章夫(KOJIMA, Akio)[JP/JP]
〒572-0039 大阪府寝屋川市池田3-9-7-205 Osaka, (JP)
桑原康浩(KUWAHARA, Yasuhiro)[JP/JP]
〒570-0003 大阪府守口市大日町3-32-11-603 Osaka, (JP)
渡辺辰巳(WATANABE, Tatsumi)[JP/JP]
〒619-0232 京都府相楽郡精華町桜ヶ丘3-32-8
エルミネンス桜ヶ丘101 Kyoto, (JP)

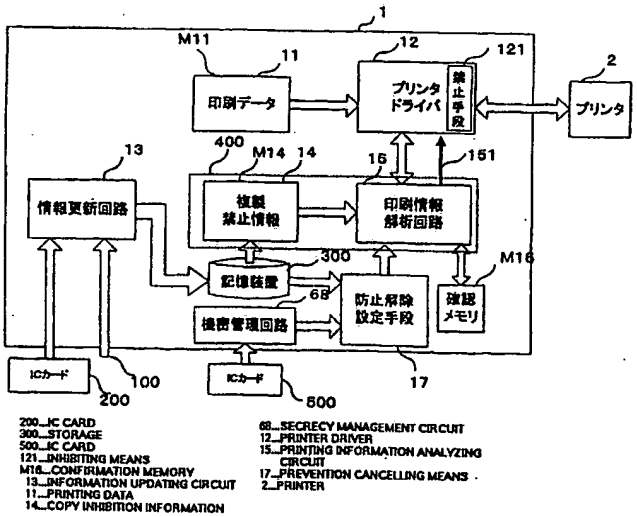
(74) 代理人
福井豊明(FUKUI, Toyoaki)
〒540-0026 大阪府大阪市中央区内本町2丁目1番19号
内本町松屋ビル10 860号 福井特許事務所 Osaka, (JP)

(81) 指定国 JP, US

添付公開書類
国際調査報告書

(54)Title: DATA MONITORING METHOD, DATA MONITORING DEVICE, COPYING DEVICE, AND STORAGE MEDIUM

(54)発明の名称 データ監視方法、データ監視装置、複製装置および記憶媒体



(57) Abstract

Each copy element of data being an object to be monitored such as printing data or reading data including at least one kind of copy elements is monitored according to at least one kind of copy inhibition information stored in inhibition information storage means and capable of being updated. By the monitoring, when one of the copy elements is judged to agree with the kind of copy inhibition information, input or output of the data being monitored is inhibited. Secrecy management information is given to the copy inhibition information, and a secrecy management level of a user is assigned to each user. In such a way, when the secrecy management level is higher than that of the secrecy management information, the inhibition of the input or output is canceled. An ID for tracing a device which has copied a printed matter is given to the copied printed matter so as to prevent unauthorized copies from diffusing.

(57)要約

禁止情報記憶手段に収容されるとともに更新可能な少なくとも１種の複製禁止情報に基づいて、少なくとも１種の複製要素より構成される印刷データ、閲覧データ等の監視対象データの各複製要素を監視しておき、この監視処理によって、前記各複製要素が前記複製禁止情報の１種と一致すると見なされたときに監視対象データの入力または出力を禁止する。前記複製禁止情報情報に機密管理情報を与える一方で、各ユーザに機密管理レベルを与えておく。これによって、ユーザの機密管理レベルが前記機密管理情報のレベルより高いときには、上記入力あるいは出力の禁止を解除する。更に、複製された印刷物に当該印刷物が複製された装置を追跡できるＩＤを含ませて、不正複製の拡散を防止できる。

明 細 書

データ監視方法、データ監視装置、複製装置および記憶媒体

技術分野

本発明は、複製が禁止された文書・画像データの、不正な複製を防止するデータ監視方法、及びその装置に関するものである。

背景技術

近年、ネットワーク化、デジタル化の進展によって、個々の機器がネットワークに接続されて、電子データを手軽に取得、印刷できるようになってきた。一方、ＤＴＰ（Desktop Publishing）では作成原稿データに忠実な画像形成を目的として技術開発が進められた結果、高精細な複製物が得られるようになってきた。これによって、電子データを取得し、高精細な印刷が簡単にできる環境が整いつつある。

一方で機密管理された文書に対しては複製されると機密漏洩等が問題になる。また、オリジナル原稿と区別がつかない複製物が簡単に得られると、著作物の不正使用、さらには、紙幣や有価証券などの偽造に悪用される恐れがあり、被害が大きい。

従来より、カラー複写機には紙幣等に対し偽造防止機能が搭載されていた。第１８図は従来のカラー複写機のブロック図である。第１８図において、スキャナ１１０から読み込まれた画像信号は、特定画像判定回路１２０によって複写が禁止されている紙幣や証券類の画像信号かどうかを画像特徴より判別し、複写が禁止されている場合には縮小画像、鏡像反転などの変換処理を行ってから画像を再生する等の処理をする複写防止機能を起動するようになっている。このような処

理がなされた画像データをプリンタ１３０に出力するようになっているので、複製された画像は容易に偽造物であることが見分けられるようになっている（例えば、特開平１－３１６７８３、特開平１１－２７５３５２、特開平１１－３５５５６２の画像処理装置）。

近年の傾向として紙の原稿だけでなく、電子データのままで受け渡しされる文書・画像の量も膨大な量になっている。パーソナルコンピュータによって、ネットワーク上から簡単に機密電子文書、著作物データを入手し、高速プリンタで大量に不正印刷できるという課題がある。

ところで、前記先行技術は、スキャナから読み取られた原稿の画像を判別するものであるので、スキャナから読み取られない電子データに係る前記課題には対処できない。

また、前記従来の技術は紙幣等、その偽造が著しく社会的影響が大きい、極めて限定された範囲での複製の禁止しかできなかった。ところが特定の事業所を例にとっても、機密を保持すべき電子データは種々あり、その内容は紙幣のように長時間に渡って一定ではなく、時間経過とともに変化するのが通常である。

ところが、前記従来の技術では複製禁止情報を環境に応じて自由に更新することは困難である。

更に、前記のように文書が電子データに置き代わるにつれて、事業所内の特定の機密文書もサーバに収容されることが多くなり、これらの機密文書を不特定の者が、印刷物としてあるいは単にディスプレイに表示して複製、閲覧することが可能となっている。これらの機密文書は複製、閲覧する権利のある人、ない人があり、その範囲は文書の種類によって異なっている。すなわち文書等に機密管理レベルがあり、ある特定の人に与えられた管理レベルが上記文書等のもつ管理レベルより上である場合にのみ当該文書の複製、閲覧を許可する必要があが、従来の御術では電子データの機密管理レベルまで考慮にいれた複製、閲覧の管理はで

きない。

本発明は、前記課題を解決するもので、複製が禁止された電子データの不正な複製を未然に、かつ迅速に防止するデータ監視方法およびシステムを提供することを目的とする。

また、環境に応じて複製、閲覧の禁止にかかる複製禁止情報の更新が自在なデータ監視方法およびシステムを提供することを目的とする。

更に、電子データの機密管理レベルに応じて複製の禁止あるいは許可の選択が自由にできるデータ監視方法およびシステムを提供することを目的とする。

発明の開示

本発明は上記目低を達成するために、以下の手段を採用している。すなわち、本発明は、まず、禁止情報記憶手段に収容されるとともに更新可能な少なくとも１種の複製禁止情報に基づいて、監視手段が、少なくとも１種の複製要素より構成される監視対象データの各複製要素を監視するようにしておく。次いで禁止手段が、前記監視手段による監視処理によって、前記各複製要素が前記複製禁止情報の１種と一致すると見なされたときに監視対象データの入力または出力を禁止する。これによって、複製禁止情報と一致する印刷データ等の監視対象データの複製・閲覧が禁止されることになる。

上記、複製禁止情報は更新手段を用いて、更新することが可能である。更新は更新権限のあるユーザが更新できるようにするのが好ましい。また、前記更新は可搬記憶メディアあるいは、ネットワークを介して新しい複製禁止情報を得ることによって実行することができる。

前記更新時に、更新履歴を記憶手段に保存しておいて、当該履歴情報に基づいて更新しようとする複製禁止情報が最新の情報である場合にのみ更新を実行することが望ましい。

前記複製禁止情報に加えて各複製禁止情報に対応する機密管理情報を禁止情報記憶手段に記憶しておき、当該機密管理情報とユーザの持つ機密管理レベルとに基づいて複製禁止、禁止解除を制御するようにする。これによって、複製・閲覧を禁止する必要のないときには、その機能を作用させないことができる。

上記複製禁止情報情報はネットワーク上のサーバ装置（マスタ情報記憶手段）に集約して記憶しておくことで、複製禁止処理をする各機器は当該サーバをアクセスするのみで複製禁止情報を得ることができる。ここで上記のように当該サーバ装置より可搬記憶媒体を介して各機器に複製禁止情報を移してもよいし、ネットワークを介して転送してもよい。当該サーバ装置には上記複製禁止情報に加えて各複製禁止情報に対応した機密管理情報も収容することが可能である。

本発明では、前記のように印刷データあるいは、閲覧データの複製を禁止するだけでなく、複製された印刷物を生成した機器を追跡することが可能である。すなわち、第１の特定情報抽出手段で監視対象データの生成に関与した所定の装置に固有な識別情報を抽出し、る情報付加手段で、前記監視対象データに前記識別情報を付与して新たな複製データを生成するようにする。

前記識別情報は、中央処理装置（ＣＰＵ）に付与されたチップ識別情報、装置に付与されたＩＰアドレス等が考えられる。

また、第２の特定情報抽出手段で、複製監視対象データの生成に関与したソフトウェアに固有な特定アプリケーション情報を抽出しておき、情報付加手段で、前記監視対象データに前記特定アプリケーション情報を付与して新たな複製データを生成する。前記特定アプリケーション情報は、ユーザが設定しているメールアドレスを用いるのが効果的である。

外部機器より監視対象データを受け入れ、当該監視対象データに従って複製物を生成する複製装置においては、以下のようにすると複製物の追跡ができる。すなわち、抽出手段において、前記監視対象データを解析し、該監視対象データに

関与した所定の装置を特定する固有情報を抽出し、特定情報付与手段で、前記抽出された固有情報を前記監視対象データに付与するようにする。

前記固有情報としては、パーソナルコンピュータを特定できる識別番号、装置に付与されたＩＰアドレスとすると有益である。

また、抽出手段が、前記複製データを解析し、複製データに関与したソフトウェアを特定する固有情報を抽出するようにし、特定情報付与手段が前記抽出された固有情報を新たな複製データとして複製物に付与するようにしてもよい。

図面の簡単な説明

第１図は、本発明の第１の実施の形態のパーソナルコンピュータのブロック図

第２図は、本発明の第１の実施の形態のパーソナルコンピュータの使用環境の構成図

第３図は、本発明の第１の実施の形態の複製禁止情報を示した図

第４図は、本発明の第１の実施の形態の印刷情報解析回路のブロック図

第５図は、本発明の第２の実施の形態のプリンタのブロック図

第６図は、本発明の第２の実施の形態の印刷情報解析回路のブロック図

第７図は、本発明の第３の実施の形態のネットアークスキャナのブロック図

第８図は、本発明の第４の実施の形態のネットワークプリンタのブロック図

第９図は、本発明の第５の実施の形態のネットワーク上に接続された機器への登録機能説明図

第１０図は、本発明の第５の実施の形態の複製禁止情報登録装置のブロック図

第１１図は、本発明の第６の実施の形態の防止解除設定回路の説明図

第１２図は、本発明の第７の実施の形態を示す図

第１３図は、本発明の第７の実施の形態に使用する機密管理情報のテーブルを示す図

第１４図は、本発明の第８の実施の形態のパーソナルコンピュータのブロック図

第１５図は、本発明の第９の実施の形態のプリンタののブロック図

第１６図は、本発明の第９の実施の形態の印刷結果を示す図

第１７図は、本発明の第１０の実施の形態のネットワークプリンタのブロック図

第１８図は、従来のカラー複写機のブロック図

発明を実施するための最良の形態

以下、本発明の実施の形態について図面を参照しながら説明する。尚、以下の説明いおいて、複製とは所定のデータ（対象データ）に基づいて当該データと同等の印刷物を生成する場合だけでなく、前記対象データを表示装置に表示して閲覧する場合をも意味する。従って、この発明を閲覧に適用する場合には以下に用いる「印刷」を含む言葉（例えば「印刷データ」）は「閲覧」（「閲覧データ」）となる。また、ハードディスク等の不揮発性記憶媒体と、ワークメモリとを区別するために、ワークメモリの参照符号にはＭを付している。

（第１の実施の形態）

第１図は本発明の第１の実施の形態を示すブロック図であり、第２図はパーソナルコンピュータの使用環境の構成図を示すブロック図であり、第３図は以下に説明する禁止情報の例を示す図であり、更に第４図は、第１図の部分を更に詳しく表したブロック図である。

第２図に示すように、パーソナルコンピュータ１（以下、ＰＣ１と記述する。）に種々のアプリケーション・ソフトウェアを搭載して簡易な印刷システムを構成した場合には、編集処理、画像処理（色処理）を行うことが可能となる。スキャナ３を入力手段とした場合、該スキャナによって取り込まれた画像データがＰ

Ｃ１に入力され、複製手段としてのプリンタ２はＰＣ１の印刷データに従って用紙、ＯＨＰ用紙等に印字イメージの像形成を行うことになる。

ＰＣ１がネットワーク１００に接続されている場合、ネットワーク１００上のネットワークスキャナ５から画像を取り込んだり、ネットワークプリンタ４に印刷データを転送して印刷もできるようになっている。

ＤＴＰシステムは、前記のように目的の原稿をＰＣ１に取り込むスキャナ３と、当該スキャナから取り込んだ画像に色処理、加工処理を行うＰＣ１と、当該画像を印刷するプリンタ２で構成され、前記スキャナより取り込まれる画像に変えて、ＰＣ１に搭載されたアプリケーションを使用して描かれた図形でもよいことはもちろんである。

次に、第１図を用いて、ＰＣ１が特定の印刷データ１１を印刷する場合の動作を説明する。

第１図はパーソナルコンピュータ１が特定の印刷アプリケーションの下で動作する場合の機能ブロック図である。スキャナ等を介して外部から入力された画像データ、あるいは、ＣＰ１の内部で画像生成用のアプリケーションを用いて生成された画像データは、印刷データ１１として印刷情報メモリＭ１１に収容されている。この状態でユーザより印刷指定が行われると、プリンタドライバ１２に渡される。ここで、印刷情報メモリＭ１１はワークメモリを想定しており、このワークメモリにはハードディスク等に予め記憶された印刷データ１１が渡される場合、あるいは、刷データ１１がスキャナ等から直接渡される場合等が考えられる。

プリンタドライバ１２は、ＰＣ１からプリンタ２にデータの橋渡しを行う制御プログラムとして、予めインストールされているものである。このプリンタドライバ１２はアプリケーションより印刷指定された印刷データ１１をプリンタ２に転送する。

第１図において、データ監視手段４００は印刷情報解析回路１５と複製禁止情

報１１を収容する禁止情報メモリＭ１４とより構成されている。尚、禁止情報メモリＭ１４には、後述するハードディスク等の禁止情報記憶手段３００より必要に応じて複製禁止情報が渡されるようになっている。尚、この複製禁止情報１４は、文書、紙幣、証券、金券などあらゆる印刷物を対象に、印刷情報を特定できるものであれば何でもよい。また、その種類は１種類に限らず、後述するように種々の種類が考えられる。更に、前記印刷情報メモリ１１と禁止情報メモリ１４は上記印刷情報メモリＭ１１と同様ワークメモリである。

前記印刷データ１１はプリンタドライバ１２よりプリンタ２に渡されるとともに、データ監視手段４００を構成する印刷情報解析回路１５にも渡される。この印刷情報解析回路１５はプリンタ２に転送される印刷データ１１のページ記述言語などで記載された文字列情報、画像パターン情報、コード情報、電子透かし技術で埋め込まれた暗号情報などの複製要素を確認メモリＭ１６上に展開する。ここで展開とは必ずしもビットマップデータへの展開を意味するもではなく、プリンタが印刷可能な形式のデータを展開することを意味している。例えば、ディスプレイリストのような中間言語、文字であればアスキーコードの状態でもよい。尚、前記コード情報とはあるコード（番号、符号等）に対応する特定のパターンを意味し、後述するコード解析エンジンによって解析されることによって、前記番号、符号にデコードされる情報をいう。

更に、前記印刷情報解析回路１５はこのようにして展開された印刷データ１１の複製要素と、禁止情報メモリＭ１４に収容された複製禁止情報１４との照合および解析を行なう（後に詳しく説明）。ここで、印刷データ１１の前記複製要素が予め禁止情報メモリＭ１４に登録されている複製禁止情報１４の１つと一致していると判定された場合は、プリンタドライバ１２に対して印刷データの転送を停止させる停止命令１５１を出力する。この停止命令１５１によって、プリンタドライバ１２に備えた禁止手段１２１は、印刷データのプリンタ２への転送を停止

する。

前記の方法によって不正な印刷をＰＣ１を通過する段階で防止できることになる。

前記の複製禁止情報１４の内容は､印刷を禁止をしようとする内容に対応して、更新できるようになっている。これによって、日々変更される機密管理レベル、機密情報、日進月歩で技術開発が進歩する偽造防止技術、暗号化技術に迅速に対応できる。

すなわち、更新手段および取得手段としての情報更新回路１３には、あらかじめ更新権利者のＩＤを登録しておく一方で、ＩＣカード２００にも更新権利者であることを意味するＩＤが記録されている。この状態で、該ＩＣカード２００がＰＣ１のカード読み込み手段に挿入されると、前記情報更新回路１３がＩＣカード２００の認証を行うようになっている。

ここで、正当な更新権利者による更新行為であると認証された場合にのみ、ＩＣカード２００に保存された更新データを取得し、ハードディスク等の禁止情報記憶手段３００に既に書き込まれている内容（もちろん新規に書き込むばあいもある）複製禁止情報１４を更新する。

尚、ＩＣカード２００自体の更新は複製禁止情報１４のマスタとなる情報（マスタ禁止情報）を収容したサーバ装置（例えば第１１図に示す複製禁止登録装置６）とそれを駆動する別途のＰＣ等で実行することになる。このＩＣカード２００の更新時にはその日付（あるは更新された内容のバージョン）を更新履歴としてＩＣカードに記憶しておく。一方で、禁止情報記憶手段３００の内容が当該ＩＣカードに基づいて更新されたときにもその日付（あるは更新された内容のバージョン）を禁止情報記憶手段３００に記憶しておき、ＩＣカードの日付（バージョン）の方が新しい場合にのみ、情報更新回路１３が禁止情報記憶手段３００の内容を更新するのが好ましい。これによて、不要な更新処理を避けることができ

る（第５の実施の形態参照）。

前記更新データはネットワーク１００を経由して入手してもよい。すなわち、ネットワーク上に、複製禁止情報１４の原情報となるマスタ禁止情報を収容したサーバ装置（例えば第１１図に示す複製禁止情報登録装置６）を配設しておく。ここで、前記情報更新回路１３は、前記ネットワーク上の前記サーバ装置を定期的にあるいは必要に応じてアクセスして前記サーバ装置よりマスタ禁止情報を取得する（第５の実施の形態参照）。

尚、上記のようにネットワークを介して複製禁止情報を取得する場合も、禁止情報記憶手段３００に収容された複製禁止情報が前回更新された日付等と、前記サーバ装置上の原情報が更新された日付等に基づいて、最新の情報のみを禁止情報記憶手段３００に取り込むようにするのが好ましい。

また、ネットワーク上のサーバ装置に更新権を持つ者のＩＤを登録しておき、ネットワークを介して送られる更新者の個人ＩＤ等に基づいて、当該更新指示者が正当権利者であるか否かの判断をする構成とすることも可能である。すなわち、前記情報更新回路１３は上記ＩＣカードに登録された更新権の情報をそのユーザのＩＤとともに上記サーバ装置に転送すると、更新権のない者からの更新要求である場合はマスタ禁止情報（複製禁止情報）をＰＣ側に転送しないようにする。但し、ここで使用するＩＣカードには上記の場合と異なって、当該ＩＣカード自身に複製禁止情報を書き込む必要はない。

このように、更新機能を持つことで、複製禁止情報の更新が簡単に行え、最新の状態に内容を維持することができる。また、機器に内蔵したメモリ（ＲＯＭ）の交換が不要となるので、更新を迅速に行うことができるとともに、不正印刷の広がりの拡大を防止できる。

また、更新権利者の認証を行うことで、情報の改ざん、不正な印刷を行う者に対する防御をすることができる。

前記のようにして取得される複製禁止情報１４は複製処理時に前記禁止情報記憶手段３００から禁止情報メモリＭ１４に第３図に示すようにして収容される。

前記禁止情報メモリＭ１４のフィールドＦ１４１には、文書中のタイトル、文書中の特定文字列（例えば、機密文書の主要なキーワードなど）等の文字情報１４１が保存される。フィールドＦ１４２には、印刷情報を特定できる固有の画像パターン情報１４２が保存される。フィールドＦ１４３には、コードの解析情報（コード情報）１４３が保存される。例えば、特定のパターン（あるいは文字列）が特定のコードに対応するときには、当該パターン（あるいは文字列）とコードの対応関係の情報が保存される。

更に、フィールドＦ１４４には、著作権で保護された写真画像データに埋め込まれた電子透かし解読情報や、スキャナ３で読み込む原稿に予め所定の暗号化(セキュリティー印刷等)によって印刷されている暗号パターンの解読アルゴリズム、コードの種別情報などの暗号情報１４４が保存される。

この複製禁止情報１４は、必要な情報を追加するだけで、あらゆる文書、原稿に対応できる。また、出力手段としてプリンタではなく表示装置を用いた場合にも適用できる。

例えば、ＣＲＴ等のディスプレイを用いた表示システムに本発明のデータ監視方法を適用する際には、前記各複製禁止情報に加えて閲覧（複製）禁止に係る静止画情報あるいは動画像情報に埋め込まれた特定の図形、コード等を複製禁止情報として追加することで足りる。

次に、印刷情報解析回路１５は第４図に示すように、プリンタドライバ１２を常に監視し、印刷を開始する際に必ず所定の動作を行うようにする。

まず、印刷情報解析回路１５が動作を開始すると、描画エンジン１５４は、プリンタドライバ１２から印刷データ１１を構成する複製要素を入手し、確認メモリＭ１６に当該複製要素に従って、各複製要素の描画処理を行う。このように、

確認メモリＭ１６に描画された各複製要素１６１は、各種の解析エンジンによって、内容が解析される。

すなわち、確認メモリＭ１６に展開された対象データ（印刷データ１１）の複製要素１６１のうち、タイトルデータがタイトル解析エンジン１５５によって抽出され、その内容の解析結果を照合回路１５９に転送する。照合回路１５９は禁止情報メモリＭ１４に収容された複製禁止情報１４の中から、照合情報として使える文字情報１４１を選び出し、前記のようにタイトル解析エンジン１５５が転送してきた解析結果と照合する。照合の結果、一致する情報が発見されると不正印刷の印字と見なし、停止命令１５１に基づいてプリンタドライバ１２の印刷動作を停止させる。

尚、前記タイトル解析エンジン１５５がタイトルを抽出する手法は種々考えられるが、一般的には、対象データの内からサイズの大きな文字が集合している領域をタイトル領域として抽出してタイトルと見なす処理をしている。

同様に、文書解析エンジン１５６は、確認メモリＭ１６に展開された複製要素からテキストデータを抽出して照合回路１５９に渡す。また、イメージ解析エンジン１５７は確認メモリＭ１６に展開された複製要素から写真部分を抽出して照合回路１５９に渡す。更に、コード解析エンジン１５８は確認メモリＭ１６に展開された複製要素をデコードして特定のコード（数値、記号）を抽出し、照合回路１５９に渡すようになっている。

前記照合回路１５９は複製禁止情報１４の中から、照合情報として使える文字（テキスト）情報１４１、画像パターン情報１４２、コード情報１４３、暗号情報１４４をそれぞれ選択し、前記の各種解析エンジンから転送されてくる解析結果と照合する。前記照合の結果、いずれかの複製禁止情報と一致する印刷情報が検出されると不正印刷と見なし、停止命令１５１によってプリンタドライバ１２の印刷動作を停止させる。

上記の照合手順において、照合回路１５９は、各解析エンジンからの問合わせに応じ、複製禁止情報１４の中から必要な情報を入手して各解析エンジンに返答するようになっている。例えば、前記、コード解析エンジン１５８が暗号の解読をするときには、デコードアルゴリズムとその鍵を必要とするが、コード解析エンジン１５８は、暗号の解読に必要なデコードアルゴリズムを照合回路１５９に問い合わせて最新の解読アルゴリズムを、上記禁止メモリＭ１４から入手して、暗号を解読をする。また、特定のコードを正規の情報に変換するときも、当該コードと対応する正規情報との対応関係が必要であるが、この場合も照合回路１５９が当該対応関係を上記禁止メモリＭ１４から入手してコード解析エンジン１５８に渡すようになっている。

このように、複数の解析エンジンを有することで、文書特徴の異なる様々な印刷原稿に対応できる。

本願発明のデータ監視装置に、機密管理機能を与えると更にその効果を有効にすることができる。

ネットワークを介しての機密管理機能は第７の実施の形態の記載に譲るとして、ここではデータ監視装置のみで実行される機密管理機能について説明する。

すなわち、各複製禁止情報に機密管理のレベルを示す機密管理情報６７を例えば第１３図に示すように与えておく（第１３図に内容については第７の実施の形態で説明する）。他方で、ＰＣ１のユーザに当該ユーザＩＤとともに機密管理レベルを与えておき、この内容を例えばＩＣカード５００に登録しておく。この状態で、ユーザが当該ＰＣ１を使用する前に、ＩＣカード５００を機密管理回路６８に読ませると、当該機密管理回路６８はその内容を、防止解除設定手段１７に渡す。防止解除設定手段１７は、上記のように印刷データ１１の複製要素が確認メモリＭ１６に展開されたとき、印刷情報解析回路１５で解析処理をしている複製要素の機密管理情報６７を参照して、現在のユーザが当該複製要素を複製、閲覧

できる権限を持っているか否かを判断する。これによって、複製、閲覧の権限のある者がユーザであるときには、印刷除法解析回路１５の禁止処理を解除することになる。

これによって、複製、閲覧の禁止をする必要のない場合にまで、印刷除法解析回路１５が作動することを防止できるようになっている。

尚、上記ＩＣカード５００は、上記更新権を登録したＩＣカードと共通にしてもよいが、上記更新権と機密管理レベルは別のデータとして扱うのが好ましい。上記の機密管理処理は、以下に説明するプリンタ、スキャナにも適用できることはもちろんである。

以上、第１の実施の形態によれば、ＰＣ１からプリンタに印刷を行う際に印刷内容を解析し、不正印刷を防止する機能を持たせることで、社内の機密文書の不正印刷、紙幣、金権の偽造などを未然に防ぐことができる。さらに、不正印刷情報を簡単に更新できる仕組みを持つことで、日々変更される機密管理レベル、機密情報、日新月歩で技術開発が進歩する偽造防止技術、暗号化技術に迅速に対応できる。結果、不正印刷の広がりの拡大を防止できる。

また、更新権利者の認証確認を行うことで、情報の改ざん、不正な印刷を行う者に対する改造防止ができる。また、管理レベルを持たせることもでき、機密情報の管理を様々な階層レベルで実現できる。

また、パーソナルコンピュータに不正印刷防機能を持たせる場合は、特別なハードウェアは不要で、ソストウェアのみをインストールすれば良く、低コストで実現できる。

（第２の実施の形態）

第１の実施の形態ではパーソナルコンピュータに不正印刷防止機能を組み込む場合を説明したが、ここではプリンタに不正印刷防止機能を持たせる実施の形態を説明する。

まず、第２図、第５図を用いて、プリンタ２の動作を説明する。第５図はプリンタ２のブロック図である。

プリンタ２はＰＣ１からの印刷データを受信バッファ２１で受け、コマンド解析回路２２に順次印刷データを転送する。コマンド解析回路２２は受け取った印刷データの言語、画像データフォーマットを解析する。次に、コマンド解析回路２２が解析処理をした結果、文字、図形描画を行う必要があれば、図形／文字描画回路２３に印刷データを転送する。図形／文字描画回路２３は、メモリコントローラ２５を経由して、画像メモリＭ２６に所定の描画動作を行う。同様に、コマンド解析回路２２が解析処理をした結果、写真データを展開する必要があれば、イメージ描画回路２７に印刷データを転送する。イメージ描画回路２７は、メモリコントローラ２５を経由して、画像メモリＭ２６に所定の写真データを展開する。メモリコントローラ２５は画像メモリＭ２６に所望の画像データが形成されるとプリンタエンジン２４に当該画像データを転送し、該プリンタエンジン２４は、受け取った画像データに基づいて紙に印刷を行うようになっている。

第５図において、データ監視手段４００は、印刷情報解析回路２８と複製禁止情報２９を収容する禁止情報メモリＭ２９により構成される。

前記データ監視手段４００を構成する前記印刷情報解析回路２８は、前記のように画像メモリＭ２６に展開される画像データを監視し、プリンタエンジン２４に画像データが転送される前に、画像データの内容を解析する。もし、画像データの内容が、複製禁止情報２９に保存された情報と一致した場合は、停止命令２１８が出力され、当該停止命令２１８を受けてプリンタエンジン２４に備えた禁止手段２４１が当該プリンタエンジン２４の動作を停止する。

次に、更新手段としての更新回路３０の機能は前記第１の実施の形態で説明した内容とほぼ同一であるのでここで異なる点を中心に説明する。尚、第１の実施の形態における禁止情報メモリＭ１４、情報更新回路１３が第２の実施の形態の

禁止情報メモリＭ２９、情報更新回路３０に対応する。また、禁止情報記憶手段３００としてはハードディスクでもよいが、プリンタでは記憶すべきデータが大量にある訳ではないので、フラッシュメモリ等の小容量の書き換え可能な不揮発性メモリを使用するのが好ましい。

ＩＣカード２００による更新の手順は第１の実施の形態と同じである。また、更新データはＰＣ１より入手してもよい。ＰＣ１は印刷データの他に、定期的、不定期、印刷時のいずれでもよいが、更新データをプリンタ２に転送する。この更新データは、受信バッファ２１経由して前記コマンド解析回路２２が受ける。このときコマンド解析回路２２は印刷データと別に定義された命令コードから更新データ２２１を検出し、当該更新データ２２１を更新回路３０に転送する。

前記ＰＣ１より得られる更新データは、ネットワーク１００を介してＰＣ１が取得するものであっても、可搬記憶媒体からＰＣ１が取得するものであってもよい。この場合更新権の確認はＰＣ１側でなされていることになる。

尚、この実施の形態に使用する複製禁止情報２９の内容は前記第１の実施の形態で説明した複製禁止情報１４と全く同じであるので説明を省略する。

次に、第６図に示した、印刷情報解析回路２８は第４図に示した印刷情報解析回路１５と略同じである。第１の実施の形態におけるようにＰＣ１内での処理はプリンタドライバ１２よりの印刷データを描画エンジン１５４で確認メモリＭ１６に展開する必要があるが、本実施の形態の場合は、画像メモリＭ２６にＰＣ１より転送される印刷データが展開される。

このように印刷データが展開されて以降の処理あるいは、回路は参照符号が異なるのみで、前記第１の実施の形態と同じである。

以上の構成による効果も前記ＰＣに対して本発明を適用した場合と同じであるが、ここでは動画に対する複製禁止はできない。ただ、動画の各フレームをプリンタで出力しようとした場合は前記各エンジンを稼働させることは可能である。

（第３の実施の形態）

第２の実施の形態ではプリンタに不正な複製を防止するデータ監視機能を組み込む場合を説明したが、ここではスキャナにデータ監視機能を持たせる実施形態を説明する。

第７図を用いて、ネットワークスキャナ５の動作を説明する。第７図はネットワークスキャナ５のブロック図である。

対象となる原稿（図示せず）をイメージセンサ５１によって読み取り、Ａ／Ｄ変換器５２によってデジタル画像データに変換する。ここで、画像中の文字等のエッジを強調するエッジ強調処理、カラー処理等画像処理が画像処理回路５３で行われ、ネットワークインタフェース５４（以下、ネットワークＩ／Ｆ５４と記す。）を経由して、画像データのネットワークへの転送が行われる。

データ監視手段４００は入力情報解析回路５５と複製禁止情報５６を収容する禁止情報メモリＭ５６より構成される。このデータ監視手段４００を構成する入力情報解析回路５５は複製禁止情報５６に保存された情報に基づいて印刷が禁止されている原稿かどうかの判定を行う。ここで、禁止されている原稿を検出した場合は、停止命令５５１をネットワークＩ／Ｆ５４に出力し、当該停止命令５５１を受けてネットワークＩ／Ｆ５４に備えた禁止手段５４１が画像データの出力を停止する。

禁止情報メモリＭ５６に収容された複製禁止情報５６は第３図に示す複製禁止情報１４と同様であるのでここでは説明を省略する。また、前記複製禁止情報５６は前記第１の実施の形態あるいは第２の実施の形態と同様の手順で、情報更新回路５７によって、更新可能である。該情報更新回路５７による更新手順も前記第１の実施の形態、あるいは第２の実施の形態で説明したように、ネットワーク上に接続された他の機器からネットワークＩ／Ｆ５４を経由して取得してもよいし、あるいは、着脱可能なＩＣカード２００、あるいはメモリカードからの更新

情報から取得してもよい。尚、前記第２の実施の形態と同様に、禁止情報記憶手段３００としてはハードディスクでもよいが、ネットワークスキャナでは記憶すべきデータが大量にある訳ではないので、フラッシュメモリ等の不揮発性メモリを使用するのが好ましい。

この実施の形態では上記のように、ハードディスクやフラッシュメモリを用いないで、ネットワーク上にあるサーバ（マスタ情報記憶手段）から、直接複製禁止情報を取得する場合を考察する。

スキャナ５には登録情報要求回路５８（情報取得手段）を設ける一方、ネットワーク上には第５の実施の形態で説明するように、前記複製禁止情報５６の原情報（複製禁止情報５６と内容は同じ）を収容したサーバ装置（例えば第１０図に示す複製禁止登録装置６）を配設しておく。そして、前記登録情報要求回路５８によりネットワークを経由して複製禁止情報５６を入手することができる。これによって、膨大な情報を格納するメモリを搭載する必要がなく、製品コストを削減できる。

ここで、前記ネットワーク上のサーバ装置が、特定の事業所のいずれか場所に設置されたサーバである場合を想定する。この場合、入力情報解析回路５５が原稿の読み取時に自動的に登録情報要求回路５８を起動して前記サーバ装置にアクセスし、必要な複製禁止情報５６を入手する仕組みを持つようにする。この複製禁止情報５６は当該ネットワークスキャナ５の中ではハードディスク等に収容しないで、直接ワークメモリである禁止情報メモリＭ５６に収容され、入力情報解析回路５５での比較照合に供される。

この登録情報要求回路５８の適用は、前記第１の実施の形態でのパーソナルコンピュータあるいは、第２の実施の形態でのプリンタにも適用できることはもちろんである。

なお、本実施の形態のスキャナとしては、ネットワークを介してＰＣ１に接続

される場合だけでなく、ＰＣ１に直接接続されるスキャナにも適用できることはもちろんである。

以上、第３の実施の形態によれば、ネットワークスキャナ５は、複製禁止情報５６と同様の内容を登録情報要求回路５８によってネットワークを経由して入手するので、膨大な情報を格納するメモリを搭載する必要がない。従って、プリンタやスキャナ等、通常はハードディスクを持たない機器に適用すると有益である。

禁止情報記憶手段３００を備えてＩＣメモリ２００あるいはネットワークを介して、当該禁止情報記憶手段３００の内容を更新する場合の効果は、上記第１、第２の実施の形態と同じであるので説明を省略する。

（第４の実施の形態）

第３の実施の形態ではスキャナにデータ監視機能を組み込む場合を説明したが、ここではネットワークプリンタにデータ監視機能を持たせる実施の形態を説明する。

第８図はネットワークプリンタ４のブロック図である。

ネットワークプリンタ４はネットワーク上に接続された機器から印刷データを受け取る。コマンド解析回路４２はネットワークインタフェース４１（以下、ネットワークＩ／Ｆ４１と記す。）を経由して印刷データ、命令コマンドのやりとりを行うとともに、受け取った印刷データの言語、画像データフォーマットを解析する。更に、前記コマンド解析回路４２、図形／文字描画回路４３、イメージ描画回路４７、メモリコントローラ４５は前記第２の実施の形態説明したプリンタにおける場合と参照符号が異なるのみで、機能は同じであるのでででここでは説明を省略する。

前記メモリコントローラ４５は画像メモリ４６に所望の画像データが形成されるとプリンタエンジン４４に画像データを転送する。プリンタエンジン４４は、受け取った画像データから紙に印刷を行う。

データ監視手段４００（刷情報解析回路４８＋禁止メモリＭ４９）を構成する印刷情報解析回路４８は、コマンド解析回路４２で解釈される印刷データを監視し、プリンタエンジン４４に画像メモリ４６から印刷データが転送される前に、画像データの内容を解析する。もし、画像データの内容が、禁止情報メモリＭ４９に収容された複製禁止情報４９のいずれかと一致した場合は、停止命令４８１を出力し、当該停止命令４８１を受けた、プリンタエンジン４４に備えた禁止手段４４１がプリンタエンジン４４の動作を停止する。第２の実施の形態と同様に、印刷情報解析回路４８は画像メモリ４６を監視し解析してもよい。

次に、更新回路３１は、前記の各実施の形態での更新回路３０、３１、５７と同様、禁止情報記憶手段３００に収容された複製禁止情報４９の内容を、禁止したい内容に合わせて更新できる。この複製禁止情報４９の更新方法の種類、および更新手順は前記各実施の形態で説明した内容と同じであるので、説明を省略する。尚、ネットワークプリンタは本来ネットワークに接続されたプリンタであるので、上記第３の実施の形態と同様、ネットワーク１００を介して複製禁止情報の更新を行うのが有益である。

（第５の実施の形態）

第１から第４の実施の形態ではデータ監視機能を組み込んだ装置について説明したが、ここではデータ監視機能を組み込んだ装置に対して、複製禁止情報を迅速に配信できる方法の一実施例を説明する。すなわち、上記各実施の形態で説明したＰＣ、スキャナ、プリンタはサーバ装置（複製禁止登録装置）に集約した複製禁止情報の配信を受けるようにすると、装置間で複製禁止情報を共通にすることができる。

第９図、第１０図を用いて、印刷を禁止したい情報の登録機能について説明する。第９図はネットワーク上に接続された機器への登録機能を説明する図であり、第１０図は複製禁止登録装置のブロック図である。

不正な複製を防止するためには、いかに迅速に目的とする複製物を検出し、複製を防止するかが重要である。第９図に図示する複製禁止登録装置６はネットワーク１００上に接続されたネットワークスキャナ５，ネットワークプリンタ４、パーソナルコンピュータ１、第ｎのネットワークプリンタ７に対して、複製禁止情報をネットワーク経由で配信する装置である。

各装置に組み込まれた不正印刷防止機能は、個々に組み込まれた更新手段（更新回路１３、３０、３１、５７）によって、複製禁止登録装置６からの更新データを取得し、複製禁止情報の内容を最新のものに更新する。これによって、ユーザに負担をかけることなく、迅速に不正印刷の情報を各機器に伝達でき、不正な複製を未然に防止できる。

次に、第１０図を用いて、複製禁止登録装置６の詳細を説明する。第１０図は複製禁止情報登録装置のブロック図である。

第１０図において、情報設定手段６６は、例えばフロピィディスク、ＣＤ－ＲＯＭ等の記録媒体１５０より複製禁止情報の原情報であるマスタ禁止情報６５を取得する。

また、前記マスタ禁止情報６５の入力方法としては、上記可搬性の記憶媒体を用いる場合の他、キーボードから情報設定手段６６に直接入力する方法、スキャナなどから画像パターンを入力する方法が考えられる。このようにマスタ禁止情報を取得した情報設定手段６６は、当該マスタ禁止情報６５をマスタ情報記憶手段８００に書き込むことになる。もちろん既にマスタ禁止情報６５が書き込まれている場合はその内容は更新されることになる。

マスタ禁止情報６５を更新する別な方法としてネットワーク１００を経由する方法もある。この場合は、登録情報自動更新手段６４に、予め決められたデータベースを指定して更新データを入手するように設定しておく。更新記録があったときは、更新履歴情報６３（例えば更新日時、あるいは更新内容のバージョン）

を履歴記憶手段８０１に保存しておく。これによって、更新処理時にネットワーク上のデータベースの更新日と自機の更新日を比較することによって、登録情報自動更新手段６４が複製禁止情報６５を更新する必要が「ある」か、「ない」かを判定できる。この、更新周期は所定の時間間隔でもよいし、予め決められたデータベースからの通知に従ってもよい。前記マスタ情報記憶手段８００と履歴記憶手段８０１は同じハードディスクの異なる領域を使用することで足りる。

情報開示／配信手段６２は、ネットワーク１００を経由した要求（第３の実施の形態参照）に対し、マスタ情報記憶手段８００に収納されたマスタ禁止情報６５を複製禁止登録情報として転送する。また、当該複製禁止登録装置６の管理下に置かれた機器、例えばプリンタ、スキャナ、パーソナルコンピュータの更新回路１３、３１、５７からの更新要請に対してマスタ禁止情報６５を複製禁止登録情報として配信する。

尚、前記禁止情報記憶手段８００と履歴記憶手段８０１は同じハードディスクの異なる領域を使用することで足りる。

前記複製禁止登録装置６の管理下に置かれた機器として、第４の実施の形態で説明したネットワークプリンタ４を用いた場合を説明する。ネットワークプリンタ４では、更新回路３１よりネットワークを介して更新要請があったとき、情報開示／配信手段６２が作動して、禁止情報記憶手段８００に収容された複製禁止情報６５を配信する。このとき、履歴記憶手段８０１から現在禁止情報記憶手段８００に書き込まれている複製禁止情報６５の更新履歴も同時に配送される。

これを受けて、前記更新回路３１は既に禁止情報記憶手段３００に収容されている複製禁止情報４９に変えて当該複製禁止情報情報６５を書き込むことになる。このとき、更新回路３１は前回の更新処理で履歴記憶手段３０１に記憶された更新履歴情報３２と、前記更新履歴情報６３を比較して更新の必要があるか否かを判断することになる。これによって、当該ネットワークプリンタ４が起動（電源

ＯＮ）したとき等、必要に応じて、禁止情報メモリＭ４９に前記複製禁止情報４５がダウンロードされることになる。尚、禁止情報記憶手段３００と履歴記憶手段３０１は同じハードディスクの異なる領域を使用することで足りる。

また、ネットワークプリンタ４には先に第３の実施の形態（スキャナ）の場合で説明したと同様の登録情報要求回路３３（情報取得手段）が備えられることも可能である。このように、登録情報要求回路３３を備えたとき、例えば画像メモリ４６に印刷データが展開された段階で、印刷情報解析回路４８の指示に基づいて、登録情報要求回路３３が必要な複製禁止情報の要求を実行し、情報開示／配信手段６２から直接に禁止情報記憶手段８００に収容された複製禁止情報６５を取得し、禁止情報メモリＭ４９に収容することもできる。

これによって、ネットワークプリンタ側は複製禁止情報４９の保存メモリが不要になり、コストを削減できる。また、禁止印刷登録情報６５を更新すれば、ネットワークプリンタ４の複製禁止情報４９も更新されたことになるので、管理がしやすく、迅速な対応ができることになる。

前記のように更新回路３１の実行した更新記録を、更新履歴情報３２として禁止情報記憶手段３０１に保存すると、登録情報要求回路３３が無効な要求をすることを防止できる。

以上、第５の実施の形態によれば、複製禁止情報登録装置６からネットワークに接続された各機器に対し禁止印刷登録情報６５を開示／配信できるので、機器管理、機器メンテナンス、機密情報レベルの変更が行いやすい。

また、一カ所の情報変更で、ネットワーク上の管理された機器を一斉に更新することができるので、迅速に不正な複製を防止できる。

以上、ネットワークを介しての配信のみについて説明したが、上記のように一か所に集約された複製禁止情報をＩＣカード（例えば第１の実施の形態のＩＣカード２００）等に可搬記憶媒体を介して各装置に配信することでも、当該複製禁

止情報登録装置６は十分に機能する。

（第６の実施の形態）

第１１図は、データ監視機能を組み込んだ装置に対して、不正複製防止機能を解除する方法の実施形態を示すブロック図である。

装置のメンテナンス等、何らかの都合により、不正印刷の防止機能を解除したい場合がある。機能を解除する権限を有するユーザは解除命令を行うことができるＩＣカード２０１を防止解除設定回路１７に挿入する。防止解除設定回路１７は、ＩＣカード２０１の認証を行い、印刷情報解析回路１５（２８、５５）に機能停止を指示する。これによって、不正な複製を防止する機能を停止できる。

また、ネットワークから特定のパスワードが入力されたときやあるいはキーボードより特定の暗号解読の鍵が入力されたときに、印刷情報解析回路１５（２８、５５）の機能を停止するようにしてもよい。

いずれにしても、解除権限をもつユーザが特定できる方法であればよい。もちろん、防止解除設定回路１７には、ＩＣカード２０１の番号等認証に必要なデータをキーボドあるいはネットワークから登録できる機能を備えるようになっており、これによって、前記ＩＣカード２０１の認証が可能となる。これにより、組織の変更、機器の移動、機密レベルの変更等、様々な管理状態に迅速に対応できる。

以上、第６の実施の形態によれば、防止解除設定回路１７を利用することで、機器メンテナンスができる。また、防止解除設定回路１７はＩＣカードの番号等の登録機能をもつので、自在な管理を可能にする。

以上、第１～第６の実施の形態によれば、迅速に不正な複製を防止することができる。

（第７の実施の形態）

データ監視機能をもつプリンタ４において、ネットワークを介して機密管理を

行う方法の一実施例を第１２図，第１３図を用いて説明する。第１２図は機密情報管理の説明図であり、第１３図は管理情報の内容の説明図である。

第１２図において、マスタ禁止情報６５の他に、機密管理情報６７を複製禁止情報登録装置６のマスタ情報記憶手段８００に持つことによって、機密情報の管理に対して、管理する情報の更新、アクセスする人に対する表示・印刷を許可する範囲の更新、などに迅速に対応できるようになる。

この機密管理を行う方法について説明する。上記第６の実施の形態で説明したように、マスタ禁止情報６５は可搬記憶媒体あるいはネットワークを介してマスタ情報記憶手段８００に収納されている。

この状態で、特定の管理者は、まず自分が更新権限を有することを通知するために複製禁止情報登録装置６にＩＣカード７００を挿入する。複製禁止情報登録装置６の情報設定手段６６は、ＩＣカード７００の内容を読み取り、更新権限者か、そうでない人物かを確認する。更新権限者であれば、キーボード６００とモニタ６６１を用いての機密管理情報６７の入力を受け付ける。

上記情報設定手段６６は、上記のようにして入力された機密管理情報６７をマスタ禁止情報６５と対にして、例えば第１３図に示すテーブル６７０に書き込むようになっている。すなわち、テーブル６７０において情報ＩＤはマスタ禁止情報（複製禁止情報）を特定するＩＤ、許可レベルは、例えばＡ，Ｂ，Ｃの順に、また更にＡ，Ｂ，Ｃの後ろに付された数字の大きい順に機密度が高くなる符号をいう、また、所属ＩＤは前記マスタ禁止情報の管轄部署を意味し、個人ＩＤはユーザを識別するＩＤをいう。これによって、たとえば、マスタ禁止情報（複製禁止情報）Ｄ００１に対しては、Ａ００１以上の許可レベルを有する人で、かつＸ００に所属する人なら情報出力が許可される。さらに、個人でＩＤ１／ＰＷ１の人を対象として複製・閲覧を許可すると定義する。

このようにして入力された機密管理情報６７はプリンタ４側では、機密管理回

路６８によって参照される。すなわち、ユーザはプリンタ４を使用する前にＩＣカード５００を機密管理回路６８に挿入する。機密管理回路６８は、ＩＣカード５００の内容を読み取り当該ＩＣカードに登録された機密管理レベルすなわち、許可レベル、所属ＩＤ、個人ＩＤをユーザＩＤとともに読み取って保持する。

次いで、特定の印刷データをＰＣ等より受け取って画像メモリＭ４６（第８図参照）に展開した段階で、登録情報要求回路３３は実施の形態５で説明したように、ネットワークインタフェース４１を経由し、複製禁止情報６５を取得して禁止情報メモリ４９に収容するとともに、対応する機密管理情報６７もテーブル６７０より取得して防止解除設定手段１７に渡す。この防止解除設定手段１７では現在印刷情報解析回路４８で照合の対象となっている複製要素に対応する機密管理情報６７と、前記のように機密管理回路６８に保持されたユーザの機密管理レベルとを比較して、ユーザの機密管理レベルが機密管理情報６７より高いときには、ユーザが許可対象者であるとして信号４８１により、プリンタエンジン４４に対し印刷を許可し、この結果、所望の印刷物を得ることができる。

不許可対象者であれば、防止解除設定手段１７に解除指定は行わず、特定の情報に対し印刷を禁止するように設定を行う。印刷情報解析回路４８は、複製禁止情報４９により、禁止対象が特定される信号４８１を用いてプリンタエンジン４４を停止させる。

以上のように、機密情報の管理情報を登録する機能を持つことで、日々の更新を迅速に行うことができる。また、プリンタ４に機密管理機能を持たせることで、機密情報の登録装置との連携で、きめ細かい複製・閲覧制御を実現できる。許可レベルによる役職階層での複製・閲覧許可のレベル制御、所属ＩＤによる拠点、組織単位による複製・閲覧許可の制御、個人ＩＤによる特定者レベルでの複製・閲覧許可の制御など、非常にきめ細かく情報開示操作を実現できる。登録装置をネットワーク上に置けば、組織変更、レイアウト変更しても、迅速に機密情報の

管理を実現することができる。さらに、出力を禁止するデバイス情報、管理期間情報など、管理を必要とする事項について拡張できるようにしておけば、さらに良い。

なお、ＩＣカード５００による個人認証の他に、手の指紋などによる個人認証、顔の認識による個人認証、人の目の網膜の認識による個人認証でも良い。個人を特定できる方法であれば、いずれも利用できる。

また、プリンタを例に説明したが、表示装置に本発明のデータ監視機能を持たせ、機密情報管理応機能を個々の装置に付加することで、機密事項の不本意な開示を防止できる。

更に、特定のパーソナルコンピュータの表示装置に限らず、ＰＤＡ(Personal Digital Assistant)、携帯電話、ノートＰＣなどあらゆる携帯情報端末の表示装置にも、もちろん応用できる。

また、音声の出力装置（スピーカー）にも応用できる。図示しないが、機密管理情報６７として、禁止するデバイス情報を付加すれば、画像情報の表示は許可するが、音声情報の出力は禁止するなど出力メディアに対する禁止制御も可能となる。

いずれにしても、機器毎に機密情報の管理機能を持たせることで、ネットワークに接続される、あらゆる機器・端末の開示レベルを制御することができる。

前記第１～第６の実施の形態では、複製禁止情報を用いて複製を禁止する場合について説明したが、以下第８～第１０の実施の形態ではパーソナルコンピュータ、プリンタ、スキャナ等で不正複製物を出力した場合に、当該機器を特定し、迅速に追跡することができる構成を備えた実施の形態を説明する。

（第８の実施の形態）

第１４図は、機器固有の識別情報をプリンタで印刷される印刷データに付加する情報付加回路のブロック図である。

情報付加回路１８は、ＰＣ１に搭載される中央制御装置（以下、ＣＰＵと記述する。）に内蔵されるＣＰＵ識別情報１８ａを抽出し、その情報をプリンタドライバ１９に送る。プリンタドライバ１９は、印刷メモリＭ１１に収容された印刷データ１１にＣＰＵ識別情報１８ａを付加し、新たな印刷データとしてプリンタ２に出力する。ここでＣＰＵは、ＰＣ１に固有かつ唯一なものであるので、ユーザを管理する情報として有効な情報原である。

同様に、情報付加回路１８は、ＰＣ１に搭載されるアプリケーション登録情報１８ｂを各アプリケーションソフト９２から取得し、その情報をプリンタドライバ１９に送る。登録情報としては、ユーザ登録情報、メールアドレスなど装置を使用しているユーザ情報や、日付情報などである。プリンタドライバ１９は、印刷データ１１にアプリケーション登録情報１８ｂを付加し、新たな印刷データとしてプリンタ２に出力する。

アプリケーション登録情報１８ｂは、インストール時のユーザ情報、ユーザーに配布される所定の製造番号、ユーザパスワードなどである。また、アプリケーションにユーザが設定するメールアドレスは使用ユーザの所在を突き止める情報として有効であり、複製物に関与したユーザ、場所、日時を特定する情報として有効な情報原となる。また、ＰＣ１のオペレーティングシステム（以下、ＯＳと記述する。）の登録情報を用いても良く、搭載されるソフトウェアでユーザ特定、ソフトウェア特定ができるものなら何でもよい。

また同様に、情報付加回路１８は、ＰＣ１に搭載されるハードウェア情報１８ｃを抽出し、その情報をプリンタドライバ１９に送る。プリンタドライバ１９は、印刷データ１１にハードウェア情報１８ｃを付加し、新たな印刷データとしてプリンタ２に出力する。ハードウェア情報として、ＰＣ１のＣＰＵが搭載される基板情報、ネットワークインタフェース９３に設定されているＩＰアドレスを取得する。また、接続されるプリンタ２の情報をドライバより取得してもよい。

以上、第７の実施の形態によれば、機器若しくはソフトウェアの使用ユーザ、場所、日付を特定する情報を自動で検出し印刷データに付与することで、複製物の出所場所、日時、使用ユーザを追跡することができる。これによって、不正な複製物を出力した機器を迅速に突き止め、その印刷データの作成状況が証拠として残されるので、不正な複製物の拡散を抑え、機密情報の漏洩範囲を最小限にくい止める事ができる。

（第９の実施の形態）

第１５図はプリンタに追跡機能を持たせた場合のブロック図である。

プリンタ２はＰＣ１からの印刷データを受信バッファ２１で受け、コマンド解析回路２２に順次印刷データを送る。コマンド解析回路２２は受け取った印刷データの言語、画像データフォーマットを解析する。

コマンド解析回路２２は受け取った印刷データの言語、画像データフォーマットを解析すると共に、印刷データに自動的に付与される識別情報２２２（装置情報、ソフトウェア情報、ハードウェア情報等）を抽出し、特定情報付加回路８０に渡す。

次に、第１の実施の形態で説明したように、前記のようにコマンド解析回路２２が解析した結果に基づいて、図形／文字描画回路２３が画像メモリＭ２６に文字、図形の描画を実行し、また、イメージ描画回路２７が画像メモリＭ２６に写真データを写真データを展開する。

更に、前記特定情報付加回路８０は、メモリコントローラ２５を経由して、画像メモリＭ２６に識別情報２２２を所定のパターンで変調して、前記画像メモリＭ２６で展開される画像に付与する。例えば、第１６図に示すように印刷データ２６１上に特定情報コード１０００が付与される。また、直接にプリンタエンジン２４に所定のパターンを送付して紙に印刷してもよい。

メモリコントローラ２５は画像メモリＭ２６に所望の画像データが形成される

とプリンタエンジン２４に画像データを転送し、プリンタエンジン２４は、受け取った画像データから紙に印刷を行う。

以上、第８の実施の形態によれば、プリンタ２が受け取った印刷データから付与されている特定情報を抽出し、プリンタ２の内部で印刷を行う際に、印刷データ上に、更にその特定情報を自動的に付与するので、社内の機密文書の不正複製、紙幣、金権の偽造などが行われた場合に機器の追跡を行うことができる。

（第１０の実施の形態）

第１７図はネットワークに接続されたプリンタに追跡機能を持たせる場合のブロック図である。

プリンタ４はＰＣ１等からの印刷データをネットワークインターフェース４１を経由して受け、コマンド解析回路４２に順次印刷データを転送し、前記コマンド解析回路４２は受け取った印刷データの言語、画像データフォーマットを解析する。

次に、図形／文字描画回路４３による文字、図形の描画処理、イメージ描画回路４７による写真データを展開処理は前記第１の実施の形態あるいは第８の実施の形態と同じであるので説明を省略する。

特定情報付加回路８０は、ネットワークインターフェース４１からプリンタ４に付与されているＩＰアドレス２２３抽出し、メモリコントローラ４５を経由して、画像メモリ４６にＩＰアドレス２２３を所定のパターンで変調して展開画像に付与する。付与する形態は、例えば第８の実施の形態同様に、第１６図に図示するように印刷データ上に特定情報コード付与される。このＩＰアドレスは上記第９の実施の形態に示すようにコマンド解析回路４２から抽出してもよいことはもちろんである。また、直接にプリンタエンジン４４に所定のパターンを送付して紙に印刷してもよい。

メモリコントローラ４５は画像メモリ４６に所望の画像データが形成されると

プリンタエンジン４４に画像データを転送する。プリンタエンジン４４は、受け取った画像データから紙に印刷を行う。

以上、第９の実施の形態によれば、ネットワークに接続されたプリンタ４の識別情報（ＩＰアドレス）がプリンタ４の内部で印刷を行う際に、印刷データ上に、更に自動付与されるので、社内の機密文書の不正複製、紙幣、金権の偽造などが行われた場合に、この機器、どの場所で印刷されたかを簡単に特定でき、追跡を行うことができる。これにより、機密情報の拡散を防止できる。

なお、本発明の複製装置は、ＣＰＵ、ＤＳＰによるソフトウェアによって実現できる。また、専用のハードウェアによって実現してもよい。

また、機密文書管理ソフトウェアとしてデーターベース、流通システム、電子メール等の文書交換ソフトウェア、ドキュメントの配信ソフトウェアに組み込むことも、もちろんできる。

また、静止画像にとどまらず、動画画像にも同様に適用でき、動画データ管理にも応用することができる。

さらには、スキャナ、プリンタ、パーソナルコンピュータ上で、原稿画像データ、文書テキストデータ、暗号データなど様々な特徴のデータに対応できることから、印刷に限らず、モニター表示にも利用できる。

以上のように、本発明によれば、複製禁止情報を更新可能としたので、原稿、電子データ等の不正な複製・閲覧を未然に、かつ迅速に防止することができる。更に、機密管理機能を備えるようにしたので、特定のユーザに与えられた機密管理レベルとの関連で、複製・閲覧か許可されるユーザに対しては上記の禁止をかけないようにきる効果がある。

更に、印刷データに該印刷データガ処理された機器の識別が可能な情報を追加することによって、不正に複製された複製物の出所を追跡することが可能となる。

尚、上記の各実施の形態における各手段はハード構成でも実現可能であるが、

ＣＰＵと該ＣＰＵに搭載されるプログラムとを用いても実現可能である。

産業上の利用可能性

上記したように本発明は、事業所の文書、図面等の不正複製・閲覧の防止に適用できる。また、同一事業所であてっても、特定の情報を複製・閲覧が許可されたユーザと許可されていないユーザの区別ができる。更に、より一般的に紙幣、金券等の複製の禁止、複製物を生成した装置の追跡に適用できる。

請求の範囲

1. 禁止情報記憶手段に収容されるとともに更新可能な少なくとも1種の複製禁止情報に基づいて、少なくとも1種の複製要素より構成される監視対象データの各複製要素を監視する監視処理と、 前記監視処理によって、前記各複製要素が前記複製禁止情報の1種と一致すると見なされたときに監視対象データの入力または出力を禁止する禁止処理と を備えたことを特徴とするデータ監視方法。

2. 更に、前記更新処理時に更新権限を持つ者の更新処理である場合にのみ更新をする請求項1に記載のデータ監視方法。

3. 前記複製禁止情報の更新情報は、可搬記憶メディアによって提供される請求項1に記載のデータ監視方法。

4. 前記複製禁止情報の更新情報は、情報提供媒体によって提供されることを特徴とする請求項1に記載のデータ監視方法。

5. 前記複製禁止情報の更新情報は、ネットワークを介して提供されることを特徴とする請求項4に記載のデータ監視方法。

6. 更に，前記禁止情報記憶手段に収容された複製禁止情報を更新したときの更新履歴を保存する履歴保存処理と、 前記履歴情報に基づいて更新しようとする複製禁止情報が最新の情報である場合にのみ実行される前記更新処理とを備えた請求項1に記載のデータ監視方法。

7. 前記禁止情報記憶手段に前記複製禁止情報に加えて機密管理情報を記憶しておき、当該機密管理情報とユーザの持つ機密管理レベルとに基づいて複製禁止、禁止解除を制御する機密管理処理を備えた請求項1に記載のデータ監視方法。

8. 更に、ネットワーク上のマスタ情報記憶手段に前記複製禁止情報の原情報を収容した状態で、当該マスタ情報記憶手段に対して前記複製禁止情報の取得を要求する情報取得処理を備えた請求項1に記載のデータ監視方法。

9．　更に、上記マスタ記憶手段に前記複製禁止情報の原情報に加えて、各原情報の機密管理情報を登録しておき、前記情報取得処理において前記複製禁止情報と機密管理情報の取得をし、　前記取得された機密管理情報とユーザの持つ機密管理レベルに基づいて複製禁止、禁止解除の制御をする機密管理処理とを備えた請求項８に記載のデータ監視方法。

１０．更に、監視機能解除権を有する者であるか否かを確認した後に、複製を停止させる機能を解除できる解除処理を備えた請求項１に記載のデータ監視方法。

１１．更新可能な少なくとも１種の複製禁止情報を収容する禁止情報記憶手段と、　前記複製禁止情報に基づいて監視対象データから生成される少なくとも１種の複製要素を監視する監視手段と、　前記少なくとも１種の複製要素が前記複製禁止情報の１つと一致すると見なされたときに前記監視対象データの入力または出力を禁止する禁止手段と、を備えたことを特徴とするデータ監視装置。

１２．更に、複製禁止情報を更新する更新手段を備えた請求項１１に記載のデータ監視装置。

１３．前記更新手段が、前記複製禁止情報が更新権限の管理情報を属性とし、前記更新手段が更新権限を持つユーザの更新処理でない場合に更新処理に禁止をかける請求項１２に記載のデータ監視装置。

１４．前記更新情報は、可搬記憶メディアによって提供される請求項１２に記載のデータ監視装置。

１５．前記更新情報は、情報提供媒体によって取得される請求項１２に記載のデータ監視装置。

１６．前記複製禁止情報がネットワークを介して取得される請求項１５に記載のデータ監視装置。

１７．更に、前記禁止情報記憶手段の複製禁止情報を更新したときの更新履歴

を保存する履歴保存手段と、 前記更新情報の履歴のに基づいて最新の複製禁止情報を取得する前記更新手段を備えた請求項１２に記載のデータ監視装置。

１８．更に、禁止情報記憶手段に前記複製禁止情報に加えて機密管理情報を記憶するとともに、当該機密管理情報とユーザの持つ機密管理レベルとに基づいて複製禁止、禁止解除を制御する機密管理手段を備えた請求項１２に記載のデータ監視装置。

１９．更に、前記複製禁止情報の原情報を収容したネットワーク上のマスタ情報記憶手段と、 当該マスタ情報記憶手段に対して前記複製禁止情報の取得を要求する情報取得手段を備えた請求項１２に記載のデータ監視装置。

２０．上記マスタ記憶手段に前記複製禁止情報の原情報に加えて、各原情報の機密管理情報を登録するとともに、前記情報取得手段が前記複製禁止情報と機密管理情報の取得するようにし、 更に、前記取得された機密管理情報とユーザの持つ機密管理レベルに基づいて複製禁止、禁止解除の制御をする機密管手段を備えた請求項１９に記載のデータ監視装置。

２１．更に、監視機能解除権を有する者であるか否かを確認した後に、複製を停止させる機能を解除できる解除手段を備えた請求項１２に記載のデータ監視装置。

２２．監視対象データの生成に関与した所定の装置に固有な識別情報を抽出する第１の特定情報抽出手段と、 前記監視対象データに前記識別情報を付与し、新たな複製データを生成する情報付加手段と、 を備えたことを特徴とする複製装置。

２３．前記識別情報は中央処理装置（ＣＰＵ）に付与されたチップ識別情報である請求項２２に記載の複製装置。

２４．前記識別情報は装置に付与されたＩＰアドレスである請求項２２に記載の複製装置。

２５．複製監視対象データの生成に関与したソフトウェアに固有な特定アプリケーション情報を抽出する第２の特定情報抽出手段と、　前記監視対象データに前記特定アプリケーション情報を付与し、新たな複製データを生成する情報付加手段と、　を備えたことを特徴とする複製装置。

２６．前記特定アプリケーション情報は、ユーザが設定しているメールアドレスである請求項２５に記載の複製装置。

２７．外部機器より監視対象データを受け入れ、当該監視対象データに従って複製物を生成する複製装置において、　前記監視対象データを解析し、該監視対象データに関与した所定の装置を特定する固有情報を抽出する抽出手段と、　抽出した固有情報を前記監視対象データ付与する特定情報付与手段と、を備えた複製装置。

２８．前記固有情報とは、パーソナルコンピュータを特定できる識別番号である請求項２７に記載の複製装置。

２９．前記識別情報は装置に付与されたＩＰアドレスである請求項２８に記載の複製装置。

３０．外部機器より監視対象データを受け入れ、前記監視対象データに従って複製物を生成する複製装置において、　前記複製データを解析し、複製データに関与したソフトウェアを特定する固有情報を抽出する抽出手段と、　抽出した固有情報を新たな複製データとして複製物に付与する特定情報付与手段と、　を備えたことを特徴とする複製装置。

３１．前記固有情報は、ユーザが設定しているメールアドレスである請求項３０に記載の複製装置。

３２．前記固有情報は、ソフトウェアの登録情報である請求項３０に記載の複製装置。

３３．外部機器より監視対象データを受け入れ、前記監視対象データに従って

複製物を生成するネットワーク対応の複製装置において、 前記複製装置に付与されたＩＰアドレスを抽出する抽出手段と、 抽出したＩＰアドレスを新たな複製データとして複製物に付与する特定情報付与手段と、を備えたことを特徴とする複製装置。

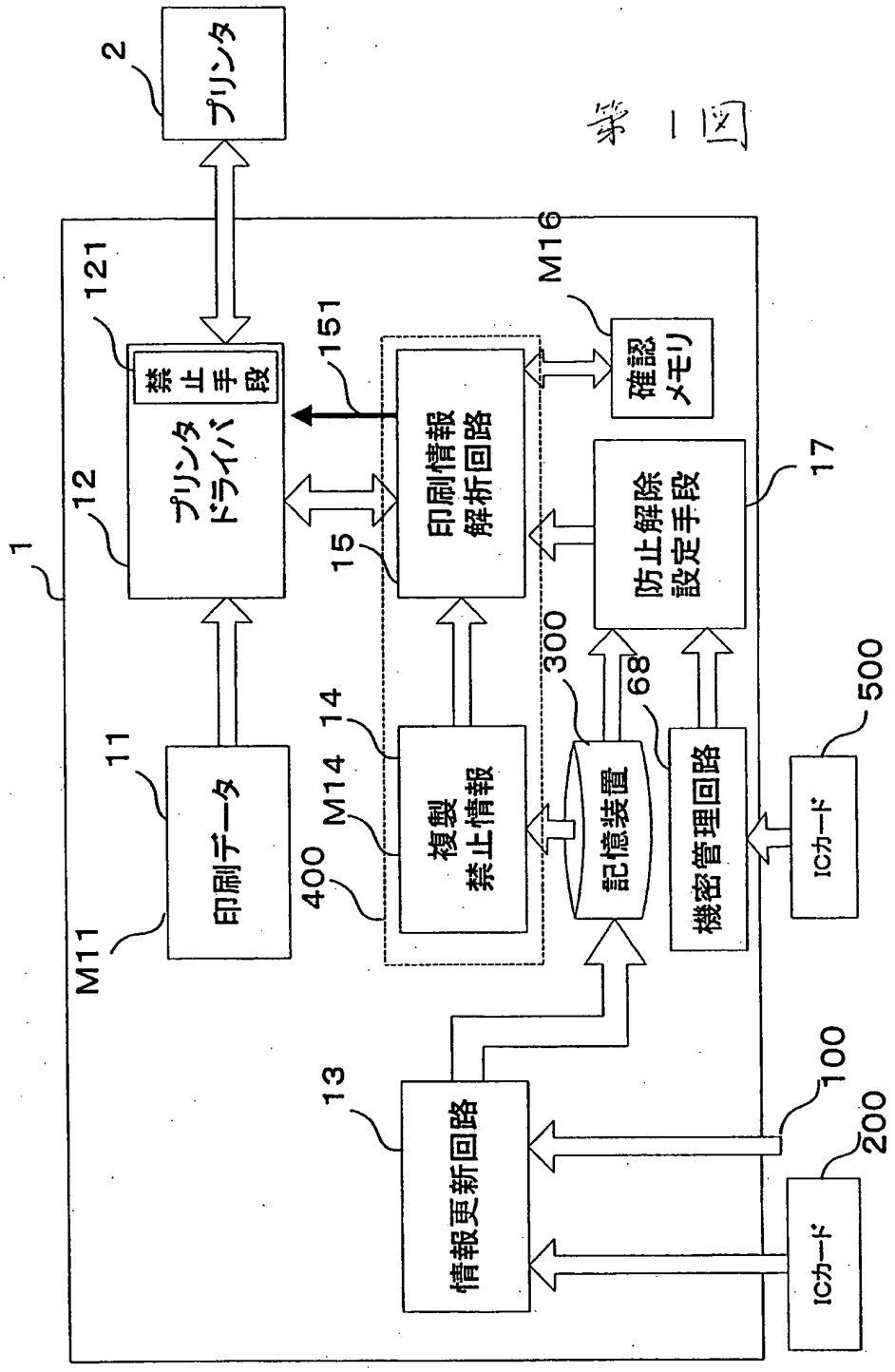
３４．禁止情報記憶手段に収容されるとともに更新可能な少なくとも１種の複製禁止情報に基づいて、少なくとも１種の複製要素より構成される監視対象データの各複製要素を監視する監視処理と、前記監視処理によって、前記各複製要素が前記複製禁止情報の１種と一致すると見なされたときに監視対象データの入力または出力を禁止する禁止処理とをプログラムとして記憶した記憶媒体。

３５．前記禁止情報記憶手段に前記複製禁止情報に加えて機密管理情報を記憶しておき、当該機密管理情報とユーザの持つ機密管理レベルとに基づいて複製禁止、禁止解除を制御する機密管理処理をプログラムとして記憶した記憶媒体。

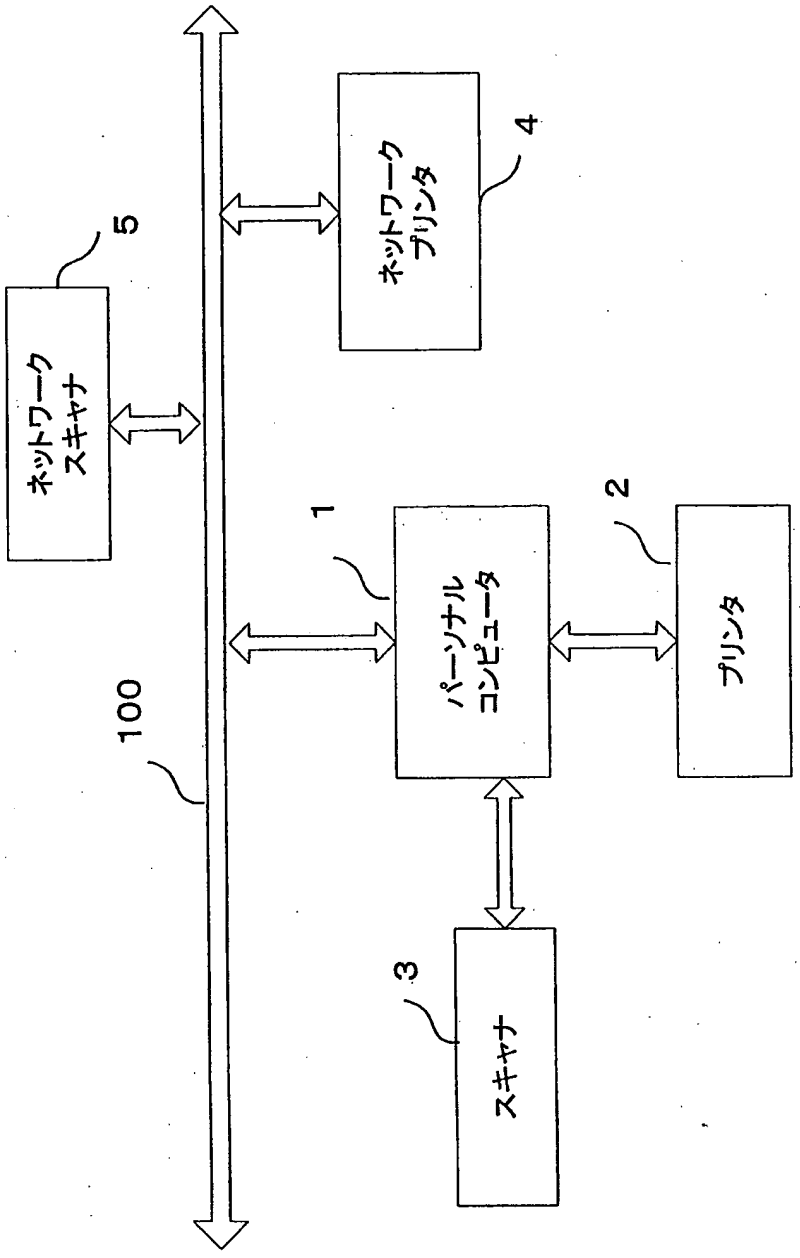
３６．外部機器より監視対象データを受け入れ、あるいは自ら監視対象データを生成して、当該監視対象データに従って複製物を生成する複製装置において、監視対象データの生成に関与した所定の装置に固有な識別情報を抽出する第１の特定情報抽出処理と、前記監視対象データに前記識別情報を付与し、新たな複製データを生成する情報付加処理とをプログラムとして記憶する記憶媒体。

３７．外部機器より監視対象データを受け入れ、あるいは自ら監視対象データを生成して、当該監視対象データに従って複製物を生成する複製装置において、複製監視対象データの生成に関与したソフトウェアに固有な特定アプリケーション情報を抽出する第２の特定情報抽出処理と、前記監視対象データに前記特定アプリケーション情報を付与し、新たな複製データを生成する情報付加処理とをプログラムと記憶する。

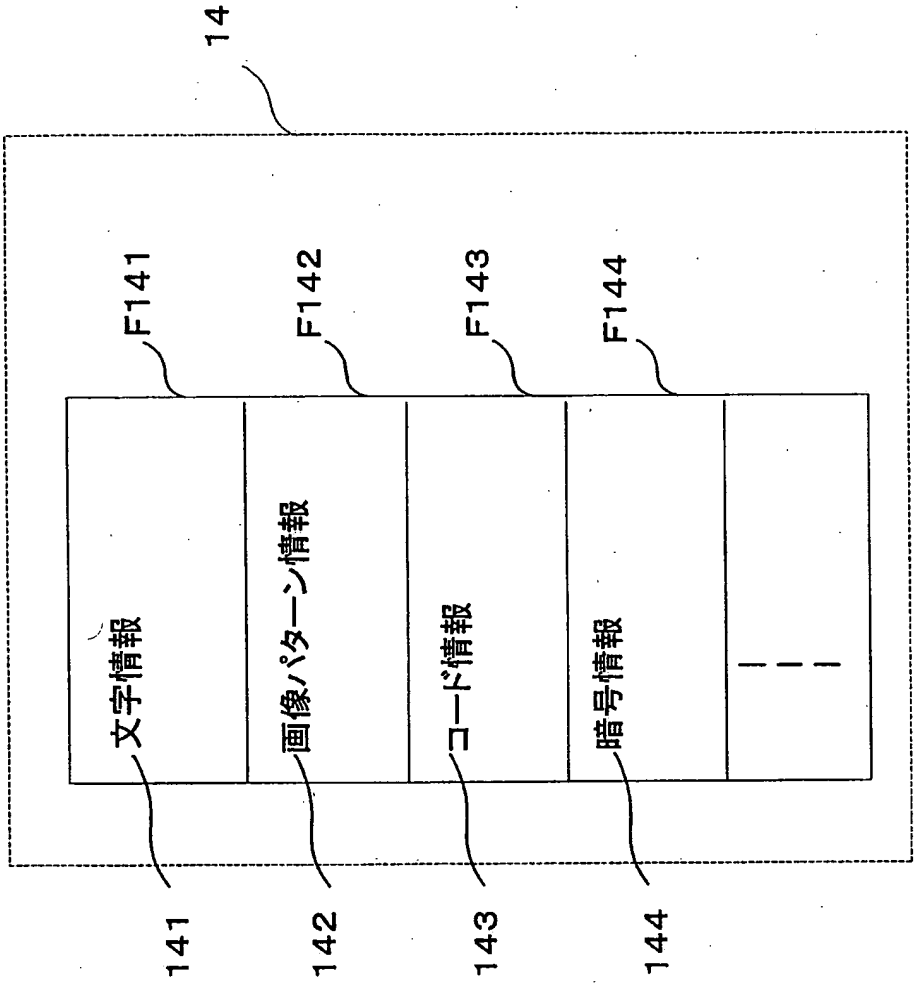
第 1 図

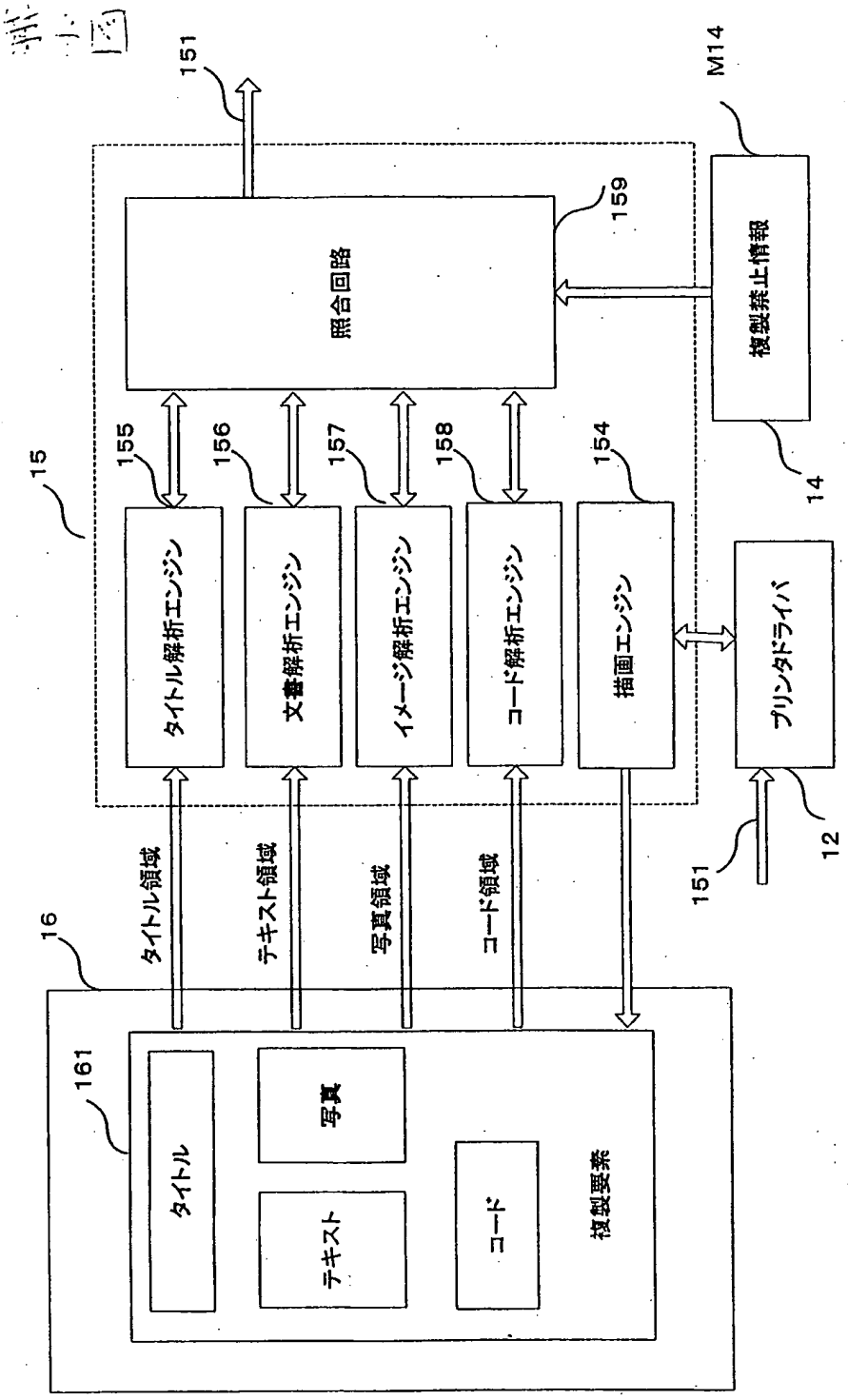

プリンタ
2
1
121
禁止手段
プリンタドライバ
12
151
印刷情報解析回路
15
M16
確認メモリ
防止解除設定手段
17
300
68
500
11
印刷データ
M11
14
M14
複製禁止情報
400
記憶装置
機密管理回路
ICカード
13
情報更新回路
100
200
ICカード

第二図

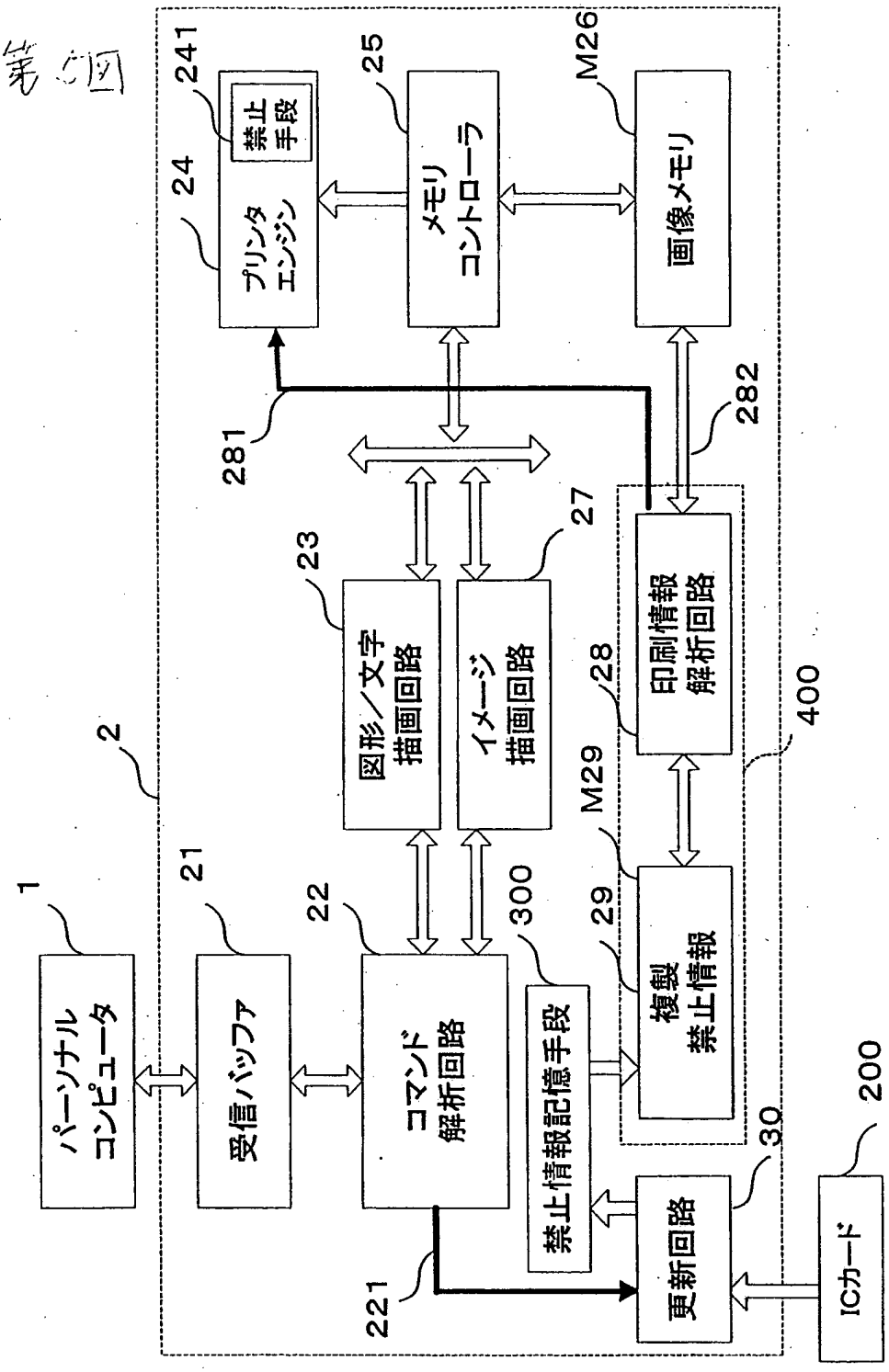


第3図

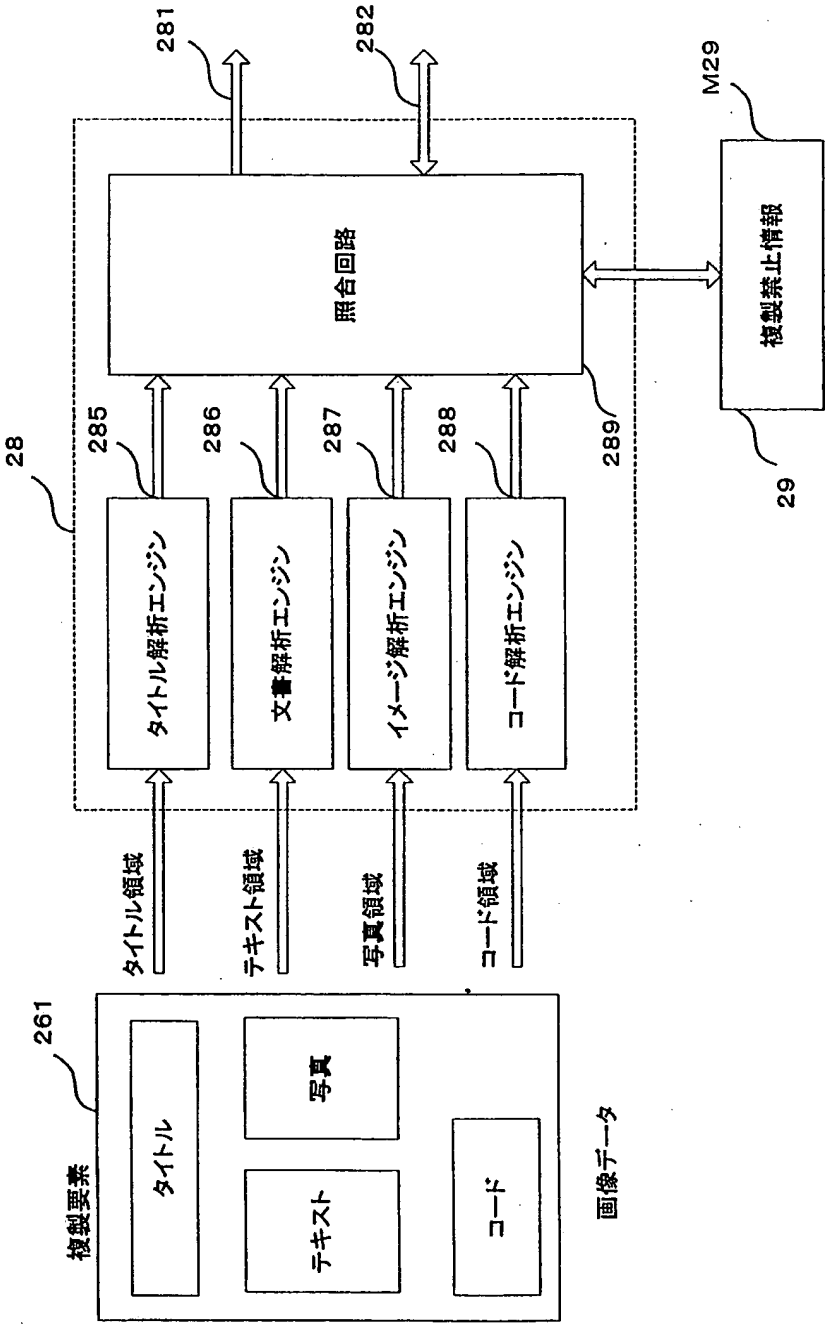

14
F141
F142
F143
F144
文字情報
画像パターン情報
コード情報
暗号情報
141
142
143
144


151
M14
159
照合回路
複製禁止情報
155
156
157
158
154
15
タイトル解析エンジン
文書解析エンジン
イメージ解析エンジン
コード解析エンジン
描画エンジン
プリンタドライバ
14
12
151
タイトル領域
テキスト領域
写真領域
コード領域
16
161
タイトル
写真
テキスト
コード
複製要素

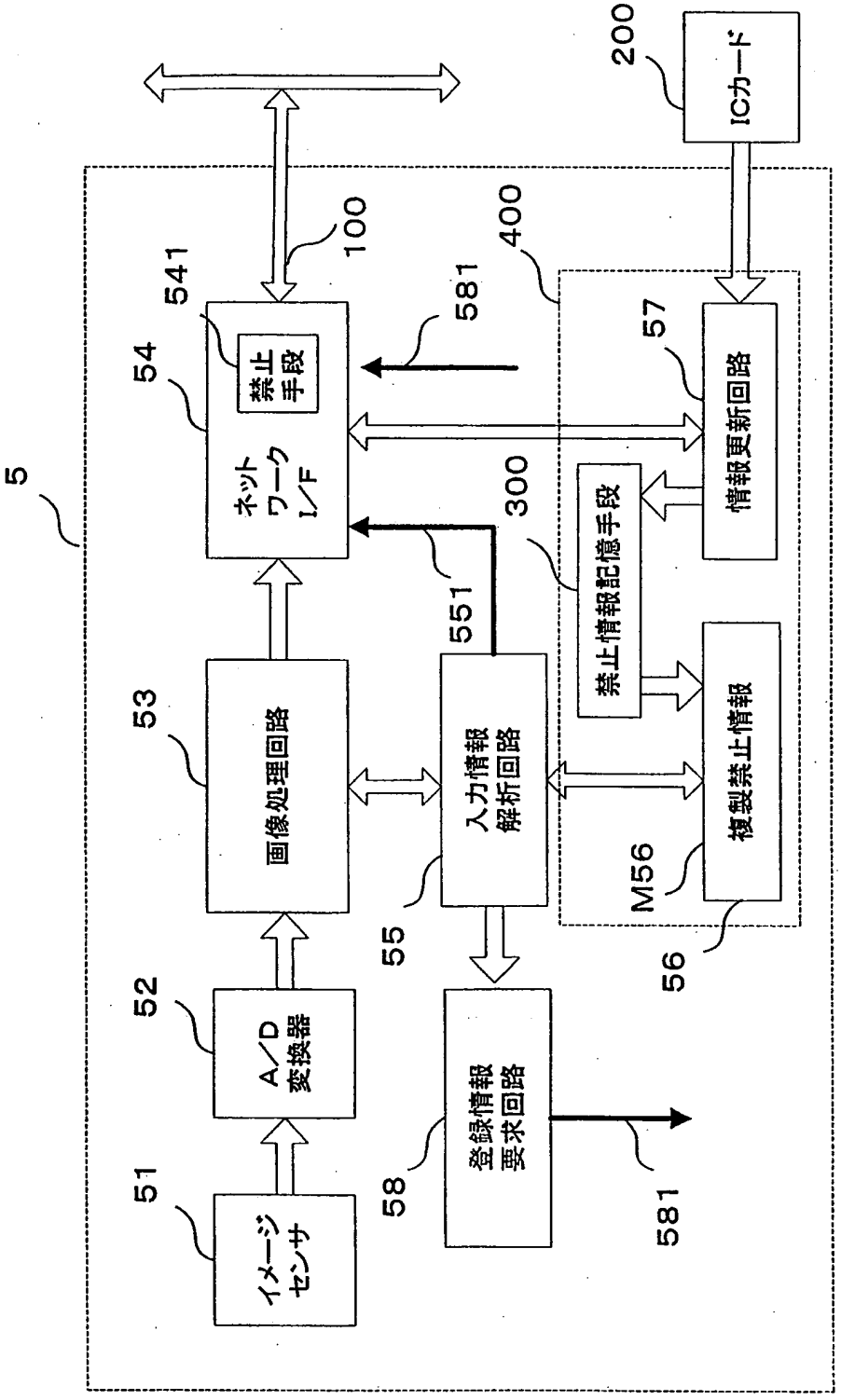
第3図


2
1
パーソナル
コンピュータ
21
受信バッファ
22
コマンド
解析回路
300
禁止情報記憶手段
221
23
図形／文字
描画回路
27
イメージ
描画回路
241
禁止
手段
24
プリンタ
エンジン
25
メモリ
コントローラ
M26
画像メモリ
281
282
400
28
印刷情報
解析回路
M29
29
複製
禁止情報
30
更新回路
200
ICカード

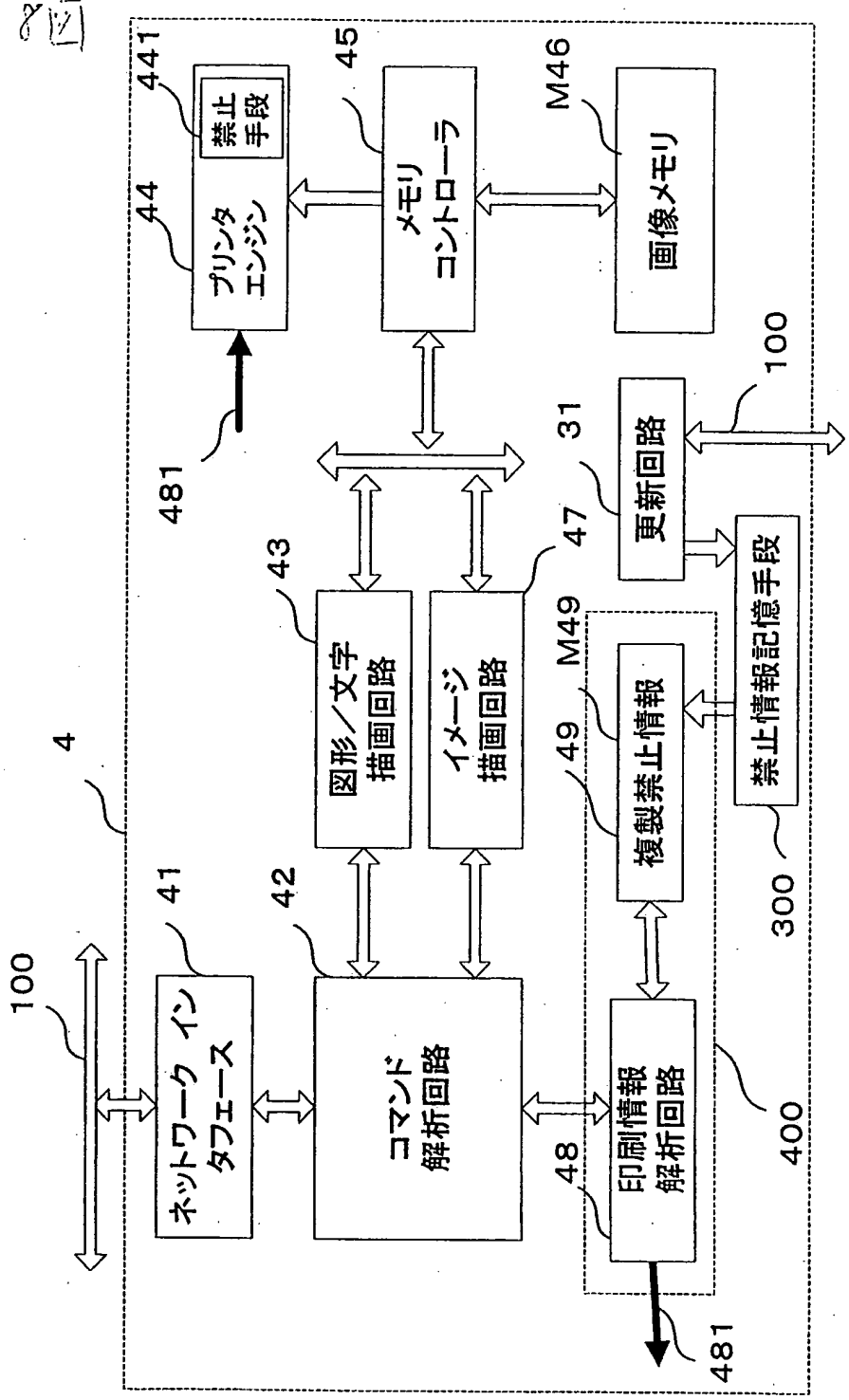
第6図


281
282
M29
照合回路
複製禁止情報
28
285
286
287
288
289
29
タイトル解析エンジン
文書解析エンジン
イメージ解析エンジン
コード解析エンジン
タイトル領域
テキスト領域
写真領域
コード領域
261
複製要素
タイトル
写真
テキスト
コード
画像データ

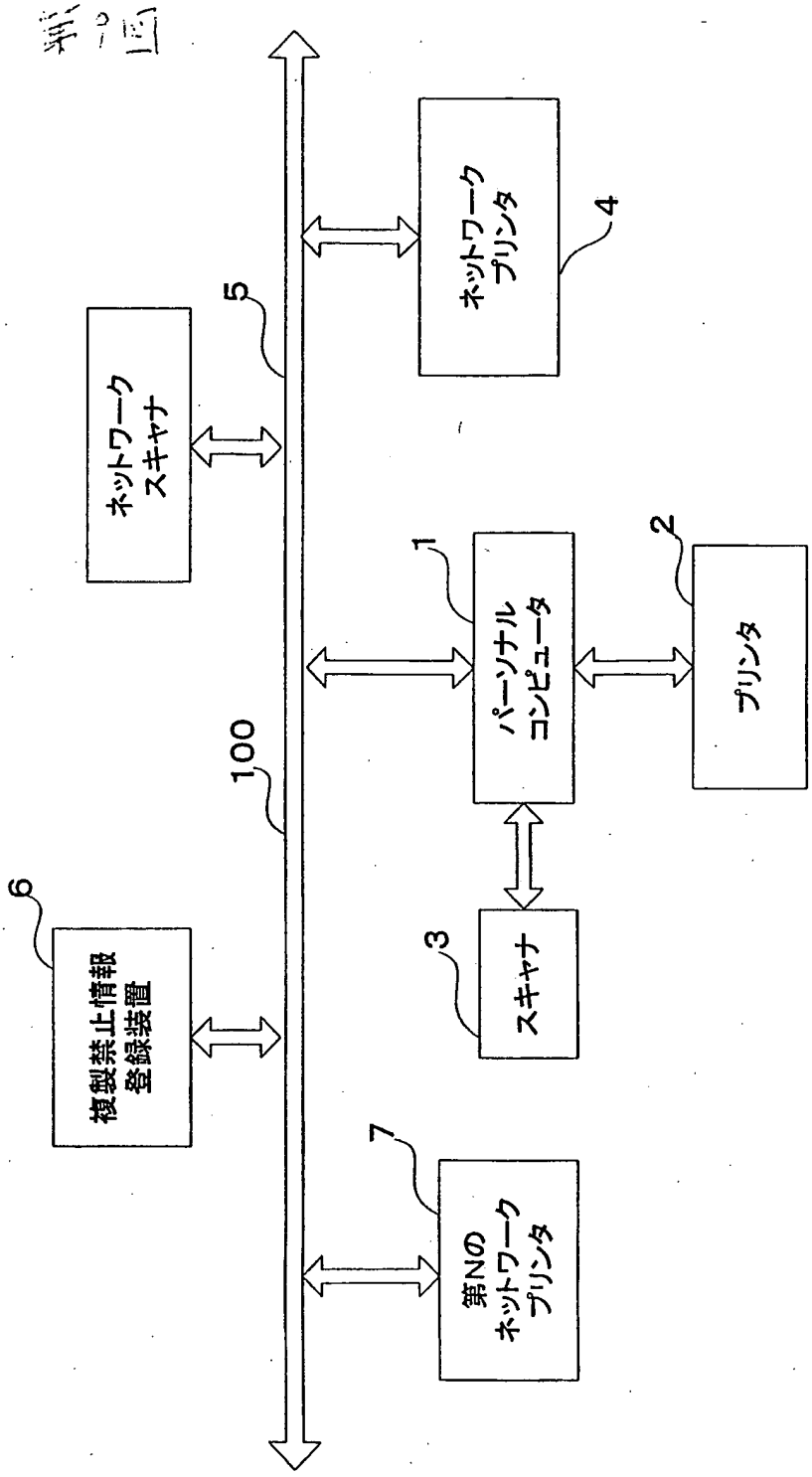
第７図


5
100
200
ICカード
400
541
581
54
禁止手段
ネットワークI/F
57
情報更新回路
300
551
禁止情報記憶手段
53
画像処理回路
入力情報解析回路
複製禁止情報
M56
55
56
52
A/D変換器
登録情報要求回路
58
581
51
イメージセンサ

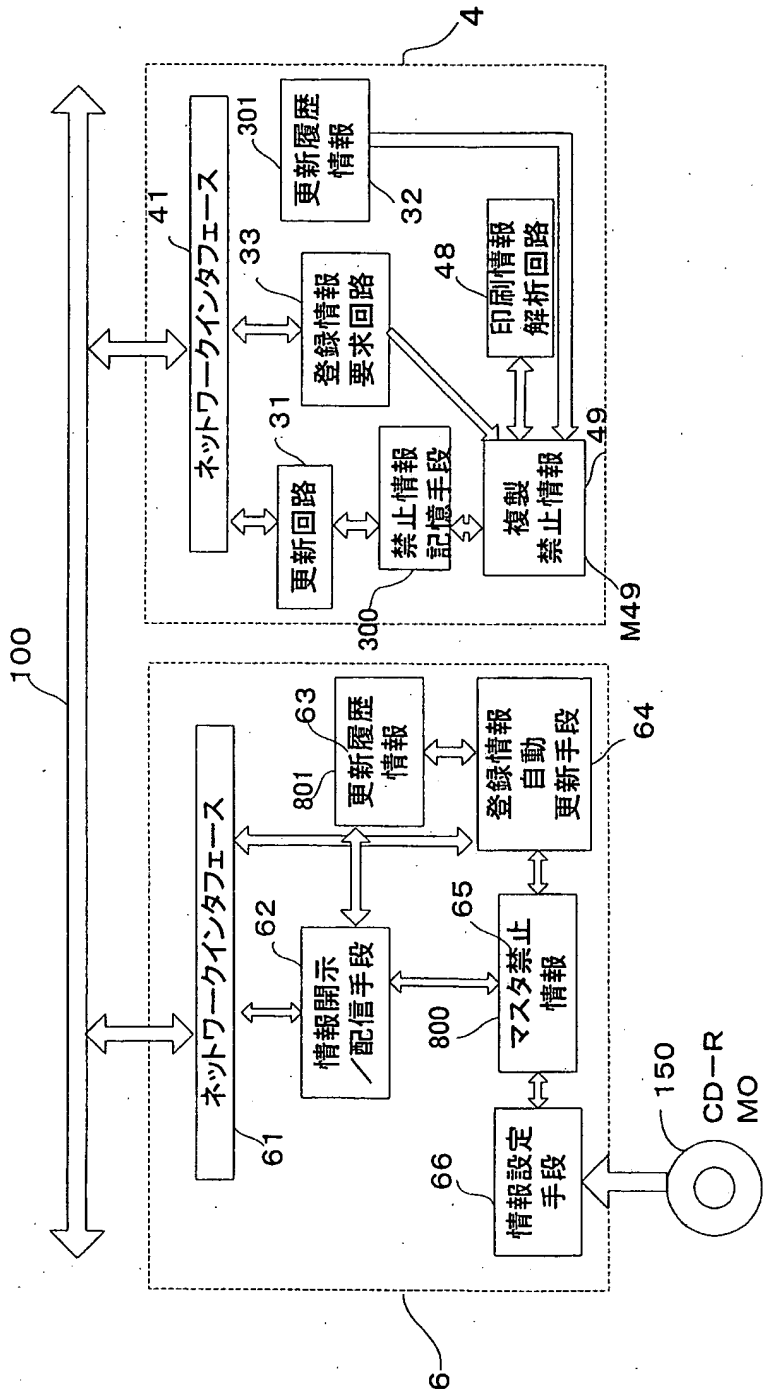
第8図


4
100
ネットワーク インタフェース
41
コマンド解析回路
42
図形／文字描画回路
43
イメージ描画回路
47
印刷情報解析回路
48
400
複製禁止情報
M49
49
禁止情報記憶手段
300
更新回路
31
100
メモリコントローラ
45
画像メモリ
M46
プリンタエンジン
44
禁止手段
441
481
481

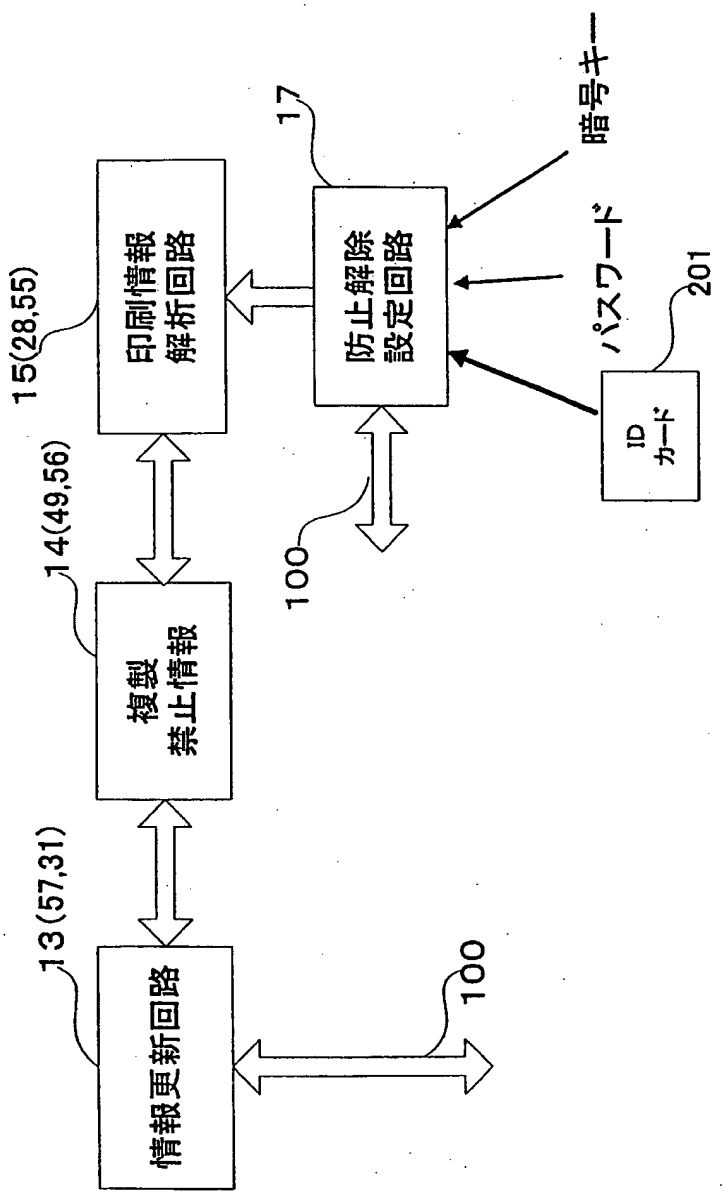
第1図


ネットワーク
プリンタ
4
5
ネットワーク
スキャナ
1
パーソナル
コンピュータ
2
プリンタ
100
6
複製禁止情報
登録装置
3
スキャナ
7
第Nの
ネットワーク
プリンタ

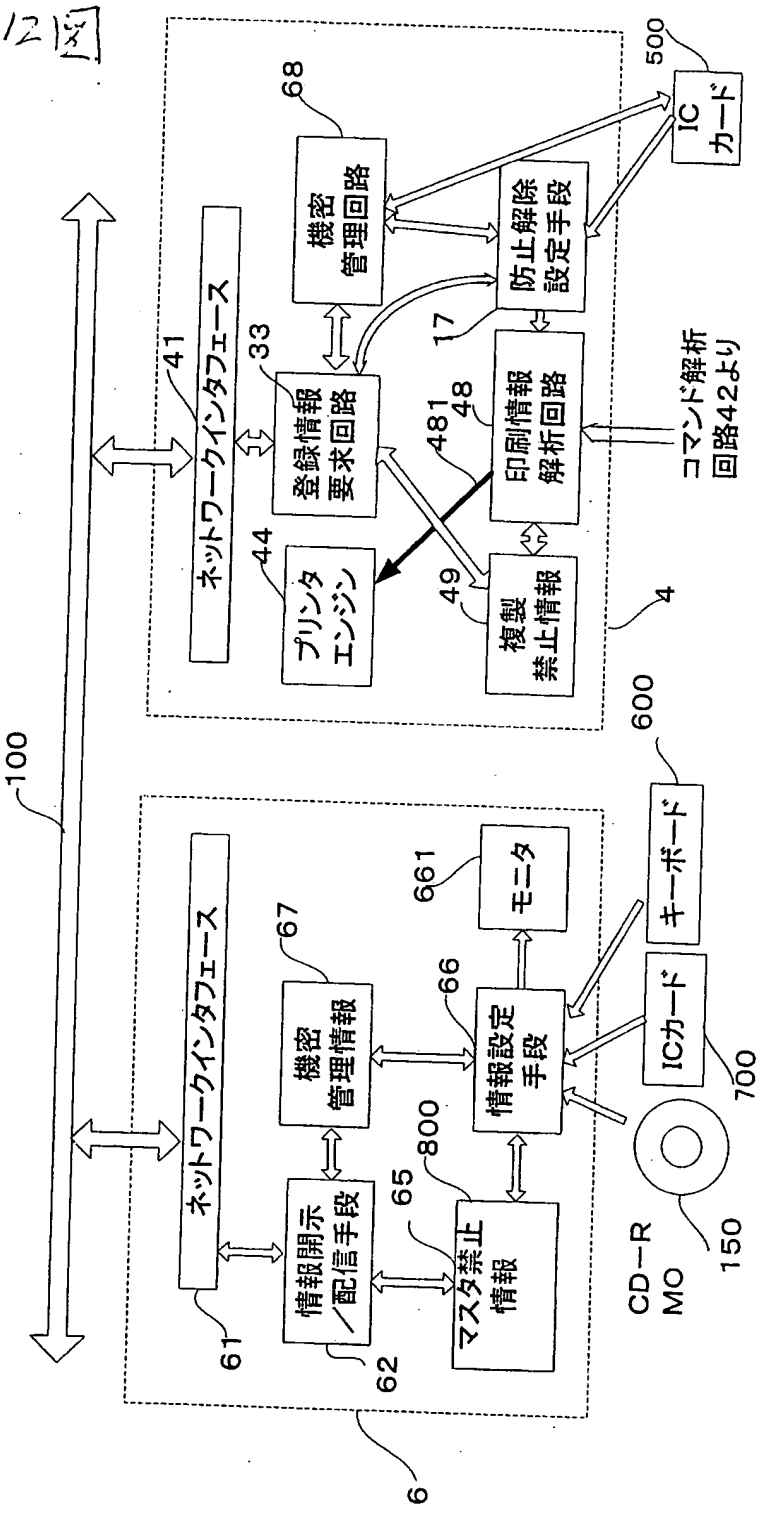
第10図


4
301
更新履歴情報
32
41
ネットワークインタフェース
33
登録情報要求回路
48
印刷情報解析回路
31
更新回路
禁止情報記憶手段
複製禁止情報
49
300
M49
100
63
801
更新履歴情報
登録情報自動更新手段
64
62
情報開示／配信手段
65
マスタ禁止情報
800
ネットワークインタフェース
61
66
情報設定手段
150
CD−R
MO
6

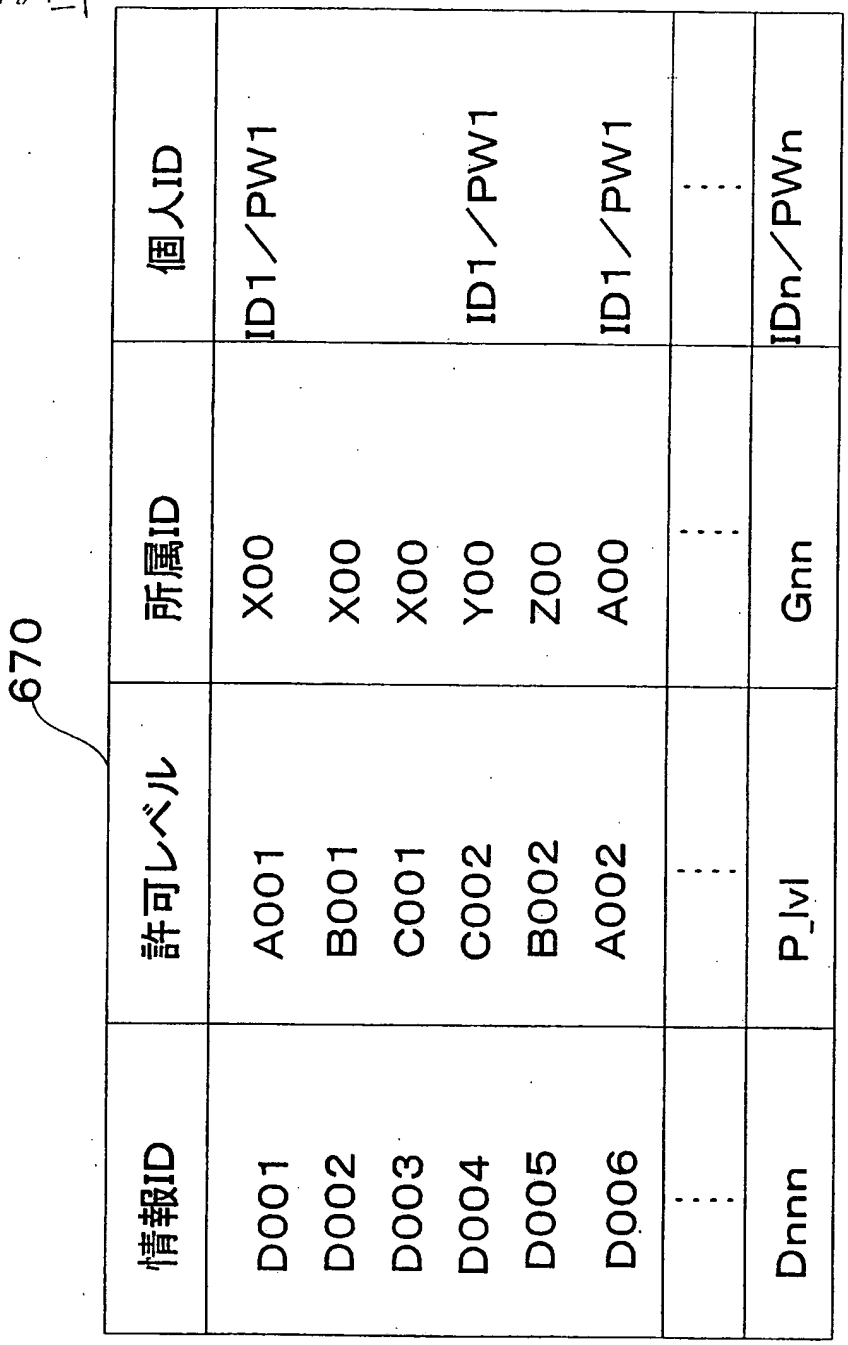
第11図

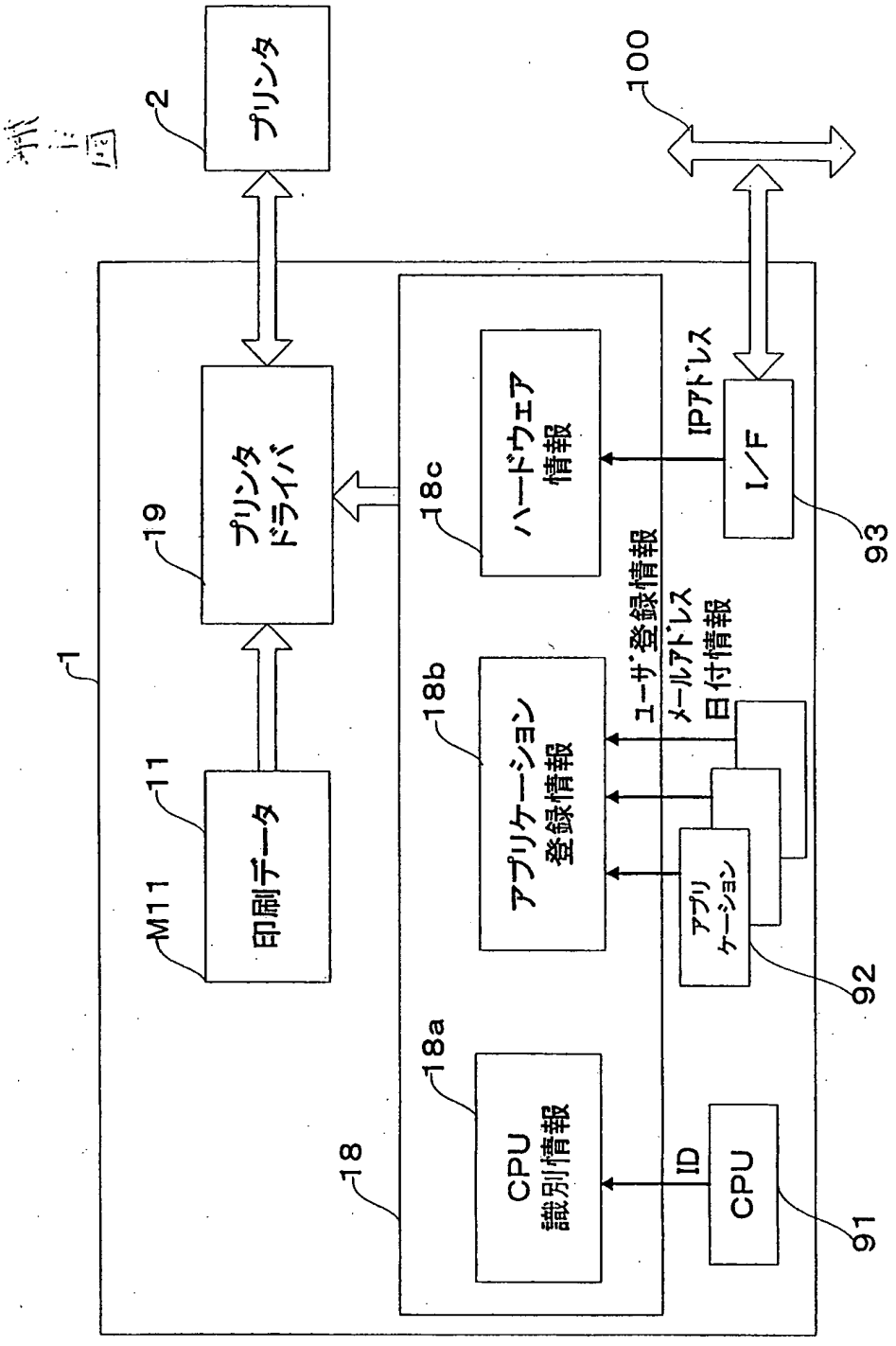

暗号キー
パスワード
201
ID
カード
17
防止解除
設定回路
印刷情報
解析回路
15(28,55)
複製
禁止情報
14(49,56)
情報更新回路
13(57,31)
100
100
100

第12図

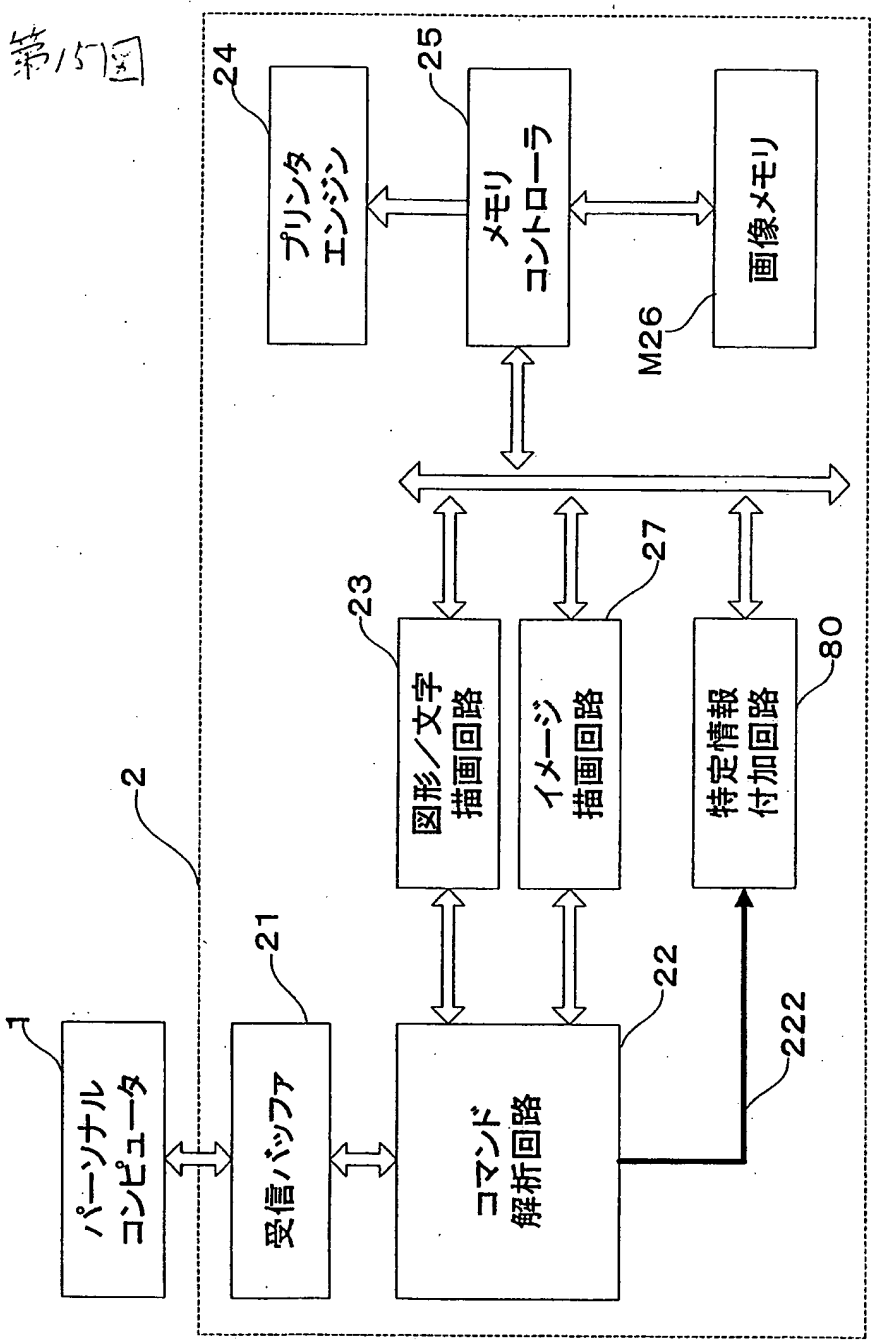

100
6
4
ネットワークインタフェース
61
情報開示／配信手段
62
機密管理情報
67
情報設定手段
66
マスタ禁止情報
65
800
モニタ
661
キーボード
600
ICカード
700
CD−R
MO
150
ネットワークインタフェース
41
登録情報要求回路
33
機密管理回路
68
防止解除設定手段
17
印刷情報解析回路
48
481
コマンド解析回路42より
プリンタエンジン
44
複製禁止情報
49
ICカード
500

第13図

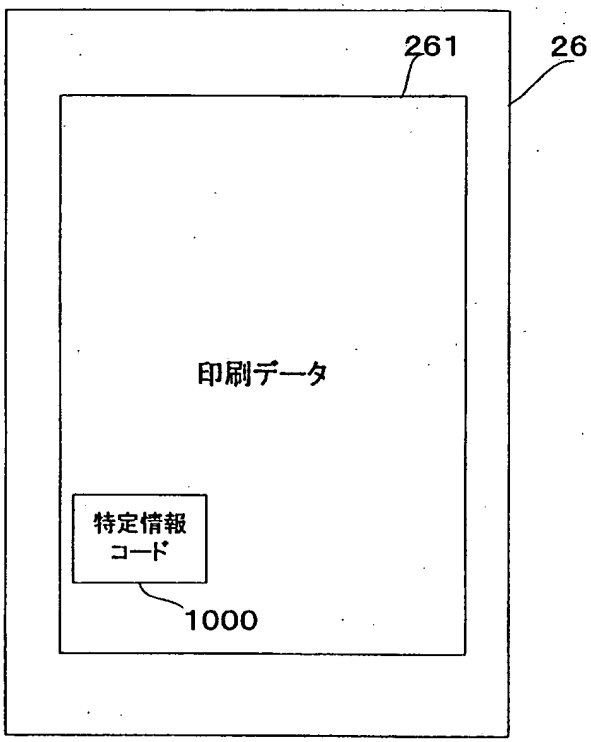

670
情報ID
許可レベル
所属ID
個人ID
D001
D002
D003
D004
D005
D006
Dnnn
A001
B001
C001
C002
B002
A002
P_lvl
X00
X00
X00
Y00
Z00
A00
Gnn
ID1／PW1
ID1／PW1
ID1／PW1
IDn／PWn


プリンタ
2
100
1
プリンタ
ドライバ
19
ハードウェア
情報
18c
IPアドレス
I/F
93
印刷データ
11
M11
アプリケーション
登録情報
18b
ユーザ登録情報
メールアドレス
日付情報
アプリ
ケーション
92
CPU
識別情報
18a
18
ID
CPU
91

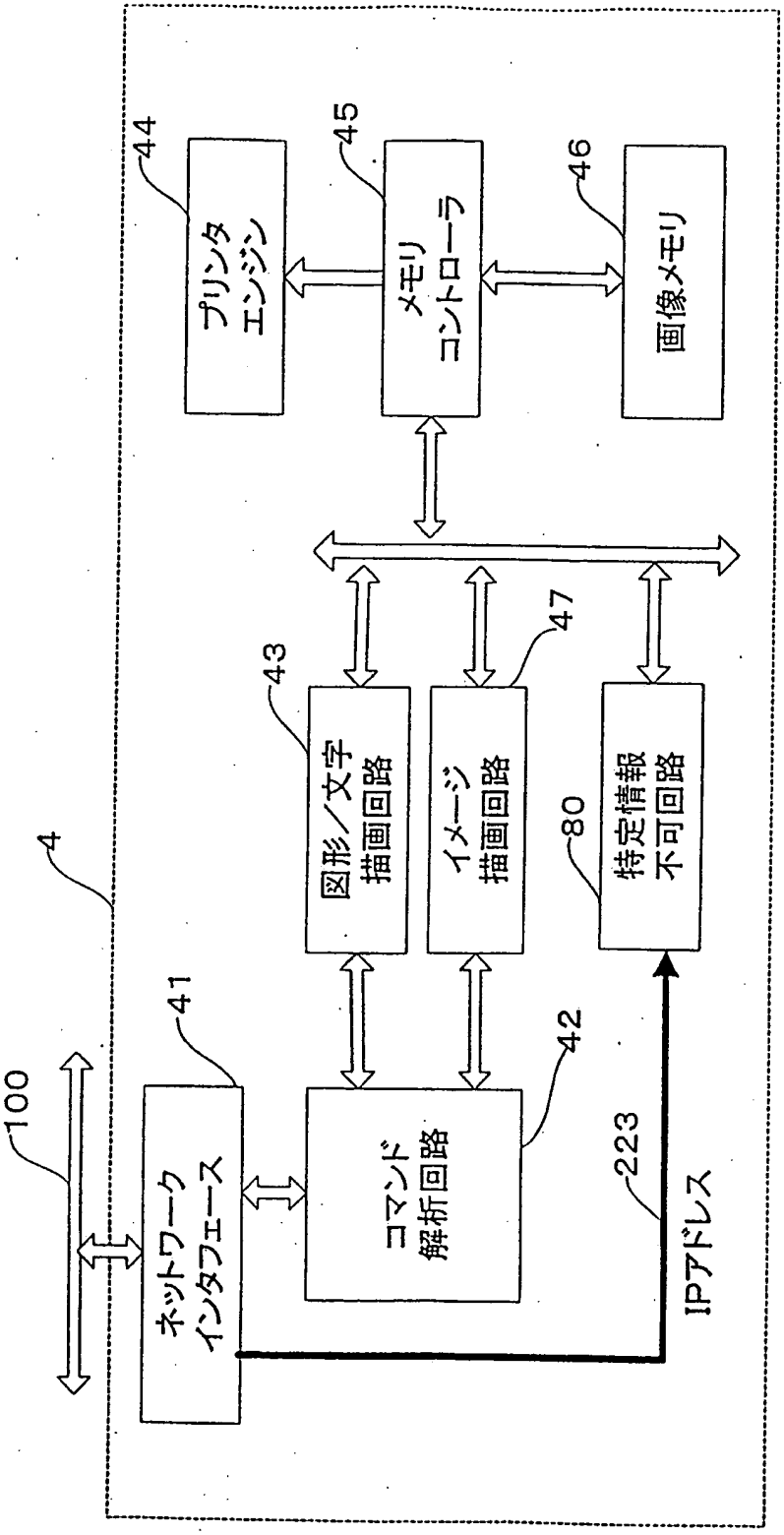
第15図


24
プリンタ
エンジン
25
メモリ
コントローラ
画像メモリ
M26
27
23
図形／文字
描画回路
イメージ
描画回路
特定情報
付加回路
80
2
21
22
222
1
パーソナル
コンピュータ
受信バッファ
コマンド
解析回路

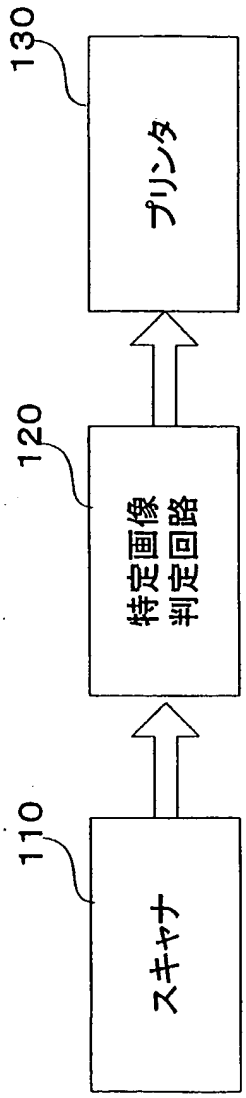
第16図



第17図


4
44
プリンタ
エンジン
45
メモリ
コントローラ
46
画像メモリ
43
図形／文字
描画回路
47
イメージ
描画回路
80
特定情報
不可回路
100
41
ネットワーク
インタフェース
42
コマンド
解析回路
223
IPアドレス

第1A図



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/01097

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.[7] H04N1/40, H04N1/387

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int. Cl.[7] H04N1/40-1/409, H04N1/46, H04N1/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1926-1996 Jitsuyo Shinan Toroku Koho 1996-2000
Kokai Jitsuyo Shinan Koho 1971-2000 Toroku Jitsuyo Shinan Koho 1994-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP, 6-178066, A (Minolta Camera Co., LTD.) 24. June. 1994 (24. 06. 94), Full text(Family: none)	1, 2, 4-6, 8, 11-13, 15, 16, 19, 22-24, 27-29, 33, 34, 36
Y		7, 9, 17, 18, 20, 25, 26, 30-32, 35, 37
X	JP, 5-282448, A (Canon Inc.) 29. October. 1993 (29. 10. 93), Full text(Family: none)	1-5, 11-16, 19, 34, 35
Y		7, 9, 18, 20
X	JP, 3-120561, A (Canon Inc.) 22. May. 1991 (22. 05. 91), Full text(Family: none)	1-4, 10-15, 21, 34

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 May, 2000 (23.05.00)	06.06.00
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/01097

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP, 5-14706, A (Canon Inc.) 22. January. 1993 (22. 01. 93), Full text(Family: none)	1-5, 11-16
X Y	JP, 3-139974, A (Canon Inc.) 14. June. 1991 (14. 06. 91), Full text(Family: none)	1-4, 11-15, 34 7, 18
X Y	JP, 6-125459, A (Ricoh Company Ltd.) 6. May. 1994 (06. 05. 94), Full text &WO, 94/09590, A1	22-24, 36 7, 9, 18, 20, 35
X	JP, 6-70134, A (Ricoh Company Ltd.) 11. March. 1994 (11. 03. 94), Full text &WO, 94/03996, A1 &GB, 2277223, A	22-24
Y	WO, 95/01043, A1 (Omron Corporation) 5. January. 1995 (05. 01. 95), Full text(Family: none)	7, 9, 18, 20
Y	JP, 2-73284, A (Canon Inc.) 13. March. 1990 (13. 03. 90), Full text(Family: none)	7, 9, 18, 20
Y	JP, 6-70150, A (Ricoh Company Ltd.) 11. March. 1994 (11. 03. 94), Full text(Family: none)	10, 21

国際調査報告

国際出願番号　PCT／JP00／01097

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl.[7] H04N1／40, H04N1／387

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl.[7] H04N1／40－1／409, H04N1／46, H04N1／60

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　1926－1996年
日本国公開実用新案公報　1971－2000年
日本国実用新案登録公報　1996－2000年
日本国登録実用新案公報　1994－2000年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP, 6－178066, A（ミノルタカメラ株式会社）24. 6月. 1994（24. 06. 94）, 全文（ファミリーなし）	1, 2, 4-6, 8, 11-13, 15, 16, 19, 22-24, 27-29, 33, 34, 36
Y		7, 9, 17, 18, 20, 25, 26, 30-32, 35, 37
X	JP, 5－282448, A（キャノン株式会社）29. 10月. 1993（29. 10. 93）, 全文（ファミリーなし）	1-5, 11-16, 19, 34, 35
Y		7, 9, 18, 20

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
23. 05. 00	06.06.00

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	田中純一	5V　9074
	電話番号　03－3581－1101　内線　3571	

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告

国際出願番号 PCT／JP00／01097

C（続き）. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP, 3－120561, A (キャノン株式会社) 22. 5月. 1991 (22. 05. 91), 全文 (ファミリーなし)	1-4, 10-15, 21, 34
X	JP, 5－14706, A (キャノン株式会社) 22. 1月. 1993 (22. 01. 93), 全文 (ファミリーなし)	1-5, 11-16
X	JP, 3－139974, A (キャノン株式会社) 14. 6月. 1991 (14. 06. 91), 全文 (ファミリーなし)	1-4, 11-15, 34
Y		7, 18
X	JP, 6－125459, A (株式会社リコー) 6. 5月. 1994 (06. 05. 94), 全文&WO, 94／09590, A1	22-24, 36
Y		7, 9, 18, 20, 35
X	JP, 6－70134, A (株式会社リコー) 11. 3月. 1994 (11. 03. 94), 全文&WO, 94／03996, A1&GB, 2277223, A	22-24
Y	WO, 95／01043, A1 (オムロン株式会社) 5. 1月. 1995 (05. 01. 95), 全文 (ファミリーなし)	7, 9, 18, 20
Y	JP, 2－73284, A (キャノン株式会社) 13. 3月. 1990 (13. 03. 90), 全文 (ファミリーなし)	7, 9, 18, 20
Y	JP, 6－70150, A (株式会社リコー) 11. 3月. 1994 (11. 03. 94), 全文 (ファミリーなし)	10, 21